# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-236622
(43)Date of publication of application : 23.08.2002

(51)Int.Cl. G06F 12/14
G09C 1/00
H04L 9/32

(21)Application number : 2001-034969
(22)Date of filing : 13.02.2001

(71)Applicant : SONY CORP
(72)Inventor : ASANO TOMOYUKI

(54) DEVICE FOR REGENERATING INFORMATION DEVICE FOR RECORDING INFORMATIONMETHOD OF REGENERATING INFORMATIONMETHOD OF RECORDING INFORMATIONRECORDING MEDIUM FOR INFORMATIONAND MEDIUM FOR RECORDING PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an information recording and regenerating device and a method therefor having a constitution wherein whether legal record content is recorded or not is determined to conduct regenerationin content regeneration.
SOLUTION: A digital signature and a public key certificate are recorded when a data is recorded in an information recording mediumto allow a recorder recorded with a content to be specified. Even when a recording medium containing the data recorded illegally is distributedthe recorder is specified to be eliminated from a system. An information regenerator confirms the reasonability of the signature and the pub ic key certificate when reading out the dataspecifys a content recoring personconfirms no presence of altering in the public key certificate and the digital signatureand regenerates thereafter the data. Use (regeneration) of the record content by the illegal recorder is efficiently eliminated by this constitution.

CLAIMS

[Claim(s)]
[Claim 1]Verification processing of an enciphered content record subject's public key certification stored in said recording medium in an information reproducing device which reproduces information from a recording medium is performedSaid

contents recording subject's public key is acquired from a public key certification in which justification was checkedAn information reproducing device performing verification processing of a contents recording subject's digital signatureand performing decoding processing of enciphered content based on an acquired this public key as a result of this verification on condition that the justification of a signature was checked.

[Claim 2]Said cipher-processing means performs verification processing of a contents recording subject's digital signature generated considering contents of enciphered content stored in said recording medium as a candidate for a signatureThe information reproducing device according to claim 1 being the composition of performing decoding processing of enciphered content as a result of this verification on condition that the justification of a signature was checked.

[Claim 3]Said cipher-processing means performs verification processing of a contents recording subject's digital signature generated considering a title key set up corresponding to enciphered content stored in said recording medium as a candidate for a signatureThe information reproducing device according to claim 1 being the composition of performing decoding processing of enciphered content as a result of this verification on condition that the justification of a signature was checked.

[Claim 4]Said information reproducing device holds a node key peculiar to each node which constitutes hierarchy key tree structure which used several different information reproducing devices as a leafand a leaf key peculiar to each information reproducing deviceSaid cipher-processing meansDecoding of validation key blocks (EKB) which consist of encryption processed data of a higher rank key by a low rank key on a path of a key tree based on a key built in said information reproducing device is performed. The information reproducing device according to claim 1 having the composition which acquires data for decryption key generation required for decoding processing of code data stored in said recording medium.

[Claim 5]The information reproducing device according to claim 4wherein said data for decryption key generation is a medium key peculiar to a common master key or a recording medium in two or more information reproducing devices.

[Claim 6]Have a cipher-processing means to perform encryption processing of contents stored in a recording medium in the Information Storage Division device which records information to a recording mediumand this cipher-processing meansThe Information Storage Division device having the composition which performs processing which generates a digital signature of a record subject of said storing contentsmatches a public key certification of enciphered contenta digital signatureand an enciphered content record subjectand is stored in a recording medium.

[Claim 7]The Information Storage Division device according to claim 6 having the composition which performs processing which said Information Storage Division device generates storing contentsa digital signatureand a management table that matched an address of a public key certificationand is stored in said recording medium.

[Claim 8]The Information Storage Division device according to claim 6wherein said cipher-processing means is the composition of performing generation processing of a contents recording subject's digital signature by making applicable to a signature contents of enciphered content stored in said recording mediummatching a generated signature with storing contents and storing it.
[Claim 9]Said cipher-processing means makes applicable to a signature a title key set up corresponding to enciphered content stored in said recording mediumand generation processing of a contents recording subject's digital signature is performedThe Information Storage Division device according to claim 6 being the composition of matching a generated signature with storing contents and storing it.
[Claim 10]Said Information Storage Division device holds a node key peculiar to each node which constitutes hierarchy key tree structure which used several different Information Storage Division devices as a leafand a leaf key peculiar to each Information Storage Division deviceSaid cipher-processing meansDecoding of validation key blocks (EKB) which consist of encryption processed data of a higher rank key by a low rank key on a path of a key tree based on a key built in said Information Storage Division device is performed. The Information Storage Division device according to claim 6 having the composition which acquires data for cryptographic key generation required for data encryption processing stored in said recording medium.
[Claim 11]The Information Storage Division device according to claim 10wherein said data for cryptographic key generation is a medium key peculiar to a common master key or a recording medium in two or more Information Storage Division devices.
[Claim 12]An information reproduction mode which reproduces information from a recording mediumcomprising:
Public key certification verification steps which perform verification processing of an enciphered content record subject's public key certification stored in said recording medium.
Said contents recording subject's public key is acquired from a public key certification in which justification was checkedSignature verification steps which perform verification processing of a contents recording subject's digital signature based on an acquired this public keyand a step which performs decoding processing of enciphered content as a result of this signature verification on condition that the justification of a signature was checked.

[Claim 13]Said signature verification steps in said information reproduction modeA step which performs verification processing of a contents recording subject's digital signature generated considering contents of enciphered content stored in said recording medium as a candidate for a signature is includedThe information reproduction mode according to claim 12 performing decoding processing of enciphered content as a result of this verification on condition that the justification of a signature was checked.
[Claim 14]Said signature verification steps in said information reproduction modeA

step which performs verification processing of a contents recording subject's digital signature generated considering a title key set up corresponding to enciphered content stored in said recording medium as a candidate for a signature is includedThe information reproduction mode according to claim 12 performing decoding processing of enciphered content as a result of this verification on condition that the justification of a signature was checked.
[Claim 15]Based on a node key peculiar to each node which constitutes hierarchy key tree structure which used several different information reproducing devices as a leaf furtherand a leaf key peculiar to each information reproducing devicesaid information reproduction modeThe information reproduction mode according to claim 12 performing processing which acquires data for decryption key generation required for decoding processing of code data which performed decoding of validation key blocks (EKB) and was stored in said recording medium.
[Claim 16]A cipher-processing step which performs encryption processing of contents stored in a recording medium in an Information Storage Division method which records information to a recording mediumAn Information Storage Division method having a step which generates a digital signature of a record subject of said storing contentsand enciphered contenta digital signature and a step that matches an enciphered content record subject's public key certificationand is stored in a recording medium.
[Claim 17]An Information Storage Division method according to claim 16 performing processing which said Information Storage Division method generates further storing contentsa digital signatureand a management table that matched an address of a public key certificationand is stored in said recording medium.
[Claim 18]An Information Storage Division method according to claim 16 said Information Storage Division method's making applicable to a signature further contents of enciphered content stored in said recording mediumand matching with storing contents a signature which performed and generated generation processing of a contents recording subject's digital signatureand storing it.
[Claim 19]Said Information Storage Division method makes applicable to a signature a title key further set up corresponding to enciphered content stored in said recording mediumand generation processing of a contents recording subject's digital signature is performedAn Information Storage Division method according to claim 16 matching a generated signature with storing contents and storing it.
[Claim 20]Said Information Storage Division method furtherDecoding of validation key blocks (EKB) is performed based on a node key peculiar to each node which constitutes hierarchy key tree structure which used as a leaf a different Information Storage Division device of plurality built in said Information Storage Division deviceand a leaf key peculiar to each Information Storage Division device.
An Information Storage Division method according to claim 16 performing processing which acquires data for cryptographic key generation required for data encryption processing stored in said recording medium.
[Claim 21]An information recording medium storing identification data of a record subject who is an information recording medium which stored enciphered

contentand recorded this enciphered contentsaid record subject's public key certificationand said record subject's digital signature.
[Claim 22]The information recording medium according to claim 21wherein said information recording medium stores further storing contentsa digital signatureand a management table that matched an address of a public key certification.
[Claim 23]It is the program storing medium which stored a computer program which makes information reproduction processing which reproduces information from a recording medium perform on computer systemsPublic key certification verification steps which perform verification processing of a public key certification of an enciphered content record subject by whom said computer program was stored in said recording mediumSaid contents recording subject's public key is acquired from a public key certification in which justification was checkedSignature verification steps which perform verification processing of a contents recording subject's digital signature based on an acquired this public keyA program storing medium having a step which performs decoding processing of enciphered content as a result of this signature verification on condition that the justification of a signature was checked.
[Claim 24]It is the program storing medium which stored a computer program which makes the Information Storage Division processing which records information to a recording medium perform on computer systemsA cipher-processing step which performs encryption processing of contents which store said computer program in a recording mediumA program storing medium having a step which generates a digital signature of a record subject of said storing contentsand enciphered contenta digital signature and a step that matches an enciphered content record subject's public key certificationand is stored in a recording medium.

---

DETAILED DESCRIPTION

---

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention An information reproducing devicethe Information Storage Division devicean information reproduction modethe Information Storage Division methodAnd about an information recording medium and a program storing mediumwhen the Information Storage Division device records data on an information recording medium especiallyan own digital signature and public key certification are recorded with dataWhen an information reproducing device reads datathe justification of the above-mentioned digital signature and a public key certification is checkedAfter checking RIBOKU [ the Information Storage Division device ]it is related with the information reproducing device considered as the composition which reads datathe Information Storage Divisior devicean information reproduction modethe Information Storage Division methodan information recording mediumand a program storing medium.

[0002]
[Description of the Prior Art]In recent yearsthe recorder and recording medium which record information in digital one are spreading with progress of digital signal processing technology and development. According to such a digital recording apparatus and a recording mediumrecord and reproduction can be repeatedwithout degrading a picture and a soundfor example. Thussince the digital data can carry out repeat execution of the copy repeatedlywith image quality or tone quality maintainedwhen the recording medium with which the copy was performed illegally will circulate in a commercial sceneprofitssuch as an owner of a copyright of various contentssuch as music and a movieor a just dealership personwill be injured. In these daysin order to prevent the unjust copy of such digital datavarious structure (system) for preventing an illegal copy is introduced into the digital recording apparatus and the recording medium.
[0003]For examplein MD (mini disc) (MD is trademark) deviceSCMS (Serial Copy Management System) is adopted as a method of preventing an illegal copy. In [ SCMS outputs a SCMS signal to the data reproduction side from a digital interface (DIF) with audio informationand ] the Data Recording Sub-Division sideIt is a system which prevents an illegal copy by controlling record of the audio information from the reproduction side based on the SCMS signal from the reproduction side.
[0004]A SCMS signal specifically. [ whether audio information is data of copy free (copy free) in which a copy is permitted any number of timesand ] It is a signal showing whether it is data in which the copy is allowed only once (copy once allowed)or it is data in which the copy is forbidden (copy prohibited). If audio information is received from DIF to the Data Recording Sub-Division sidethe SCMS signal transmitted with the audio information will be detected. And when the SCMS signal serves as copy free (copy free)audio information is recorded on a mini disc with a SCMS signal. When the SCMS signal is permitted (copy once allowed) once about the copya SCMS signal is changed into copy prohibition (copyprohibited)and it records on a mini disc with audio information. Audio information is not recorded when the SCMS signal serves as copy prohibition (copy prohibited). By performing control which uses such SCMSthe audio information which has copyright prevents being copied illegally by SCMS with a mini disc device.
[0005]Howeversince it is a premise that the apparatus itself which records data has the composition which controls record of the audio information from the reproduction side based on a SCMS signal as mentioned above as for SCMSWhen a mini disc device without the composition which performs control of SCMS is manufacturedit becomes difficult to cope with it. Thenfor examplewith the DVD playerit has the composition of preventing the illegal copy of data which has copyrightby adopting a contents scramble system.
[0006]In a contents scramble systemto DVD-ROM (Read Only Memory). A video dataaudio informationetc. are enciphered and recorded and the key (decode key) used for decoding the enciphered data is given to the licensed DVD player. It is

licensed to the DVD player designed follow predetermined regulation of not copying illegally of operation. Thereforein the licensed DVD playeran image and a sound are renewable from DVD-ROM by decoding the encryption data recorded on DVD-ROM using the given key.
[0007]On the other handsince the DVD player which has not been licensed does not have a key for decoding the enciphered datait cannot decode the encryption data recorded on DVD-ROM. Thusin contents scramble system compositionthe DVD player which does not fulfill the conditions demanded at the time of a license can reproduce DVD-ROM which recorded digital dataand an illegal copy is prevented.
[0008]Howeverthe contents scramble system adopted with DVD-ROM is aimed at the recording medium (suitably henceforth ROM media) which cannot write in the data by a user.
It is not taken into consideration about application to the recording medium (suitably henceforth RAM media) which can write in the data by a user.

[0009]That iseven if the data recorded on ROM media was encipheredwhen the enciphered data is all copied to RAM media as it waswhat is called a refreshable pirate edition will be able to be created with the licensed just device.
[0010]Thenin previous patent application and JPH11-224461A (Tokuganhei10-25310) these peopleRecord the information (it is hereafter described as medium identification information) for identifying each recording medium on a recording medium with other dataand on condition that it is the device which received the license of this medium identification informationit carries outOnly when the condition was fulfilledthe composition whose access to the medium identification information of a recording medium is attained was proposed.
[0011]The data on a recording medium is enciphered in this method by the secret key (master key) obtained by receiving medium identification information and a licenseMeaningful data cannot be obtained even if the device which has not been licensed reads this enciphered data. When a device is licensedthe operation is specified so that an unjust duplicate (illegal copy) may not be made.
[0012]Since the device which has not been licensed cannot access medium identification information and medium identification information serves as an individual value for each medium of everyEven if the device which has not been licensed reproduces all the enciphered data that is recorded on the recording medium to a new recording mediumSince the data recorded on the recording medium created by making it such cannot be correctly decoded in the licensed device as well as the device which has not been licensedan illegal copy will be prevented substantially.
[0013]By the wayas for the master key stored in the licensed devicein the above-mentioned compositionit is common in a complete aircraft machine that it is common. Thusit is because it is conditions required in order that storing a common master key to two or more apparatus may make refreshable the medium recorded by one apparatus by other apparatus (interoperability is secured).

[0014]Howeverin this methodwhen an aggressor succeeds in the attack of one apparatus and takes out a master keythe data currently enciphered and recorded in all the systems can be decodedand the whole system collapses. In order to prevent thiswhen what a certain apparatus was attacked and the master key exposed is revealedit is necessary to give the master key which updated the master key to a new thing and was newly updated by complete aircraft machines other than the apparatus which yielded to the attack. Although the peculiar key (debye skiing) is given to each apparatus as a method simple No. 1 which realizes this compositionthe value which enciphered a new master key on each debye skis is prepared and the method transmitted to apparatus via a recording medium can be consideredThere is a problem that the total amount of messages which should be transmitted in proportion to the number of apparatus increases.
[0015]As composition which solves the above-mentioned problemthese peopleVia a recorcing medium or a communication line using the key distribution method of composition of having arranged each Information Storage Division playback equipment to each wooden leaf (leaf) for n minutesWhen a key (a master key or a medium key) required for the record to the recording medium of contents data or the reproduction from a recording medium is distributed and each device is made to perform record of contents dataand reproduction using thisThe just (to device which the secret has not exposed) composition which receives and can transmit a master key or a medium key in the small amount of messages is proposed previouslyand patent application (Japanese Patent Application No. 2000-105328) has already been carried out. The key which is specifically needed in order to generate a key required for the record to a recording mediumor the reproduction from a recording mediumFor examplethe node key assigned to the node which constitutes each wooden leaf (leaf) for n minutes is set up as an updating node keyThe leaf key in which only just apparatus has an updating node keyand validation key blocks (EKB) including the information which carried out encryption processing in the mode which can decode by a node key are distributed to each Information Storage Division playback equipmentIt is the composition which made acquirable the key which each device needs for record or the reproduction from a recording medium by the EKB decoding processing of each Information Storage Division playback equipment which received validation key blocks (EKB).
[0016]
[Problem(s) to be Solved by the Invention]In the above-mentioned compositionalthough it is possible to eliminate from a system the device which the secret exposedit is necessary to specify whether for the purposeit was exposed of the secret of which device. For examplethe clone device which carries the secret of which a certain device was robbed is madeand if it can specify having been sold in the black marketthe device with which the secret was stolen will be specified and it will be eliminated from a system.
[0017]By the wayconsidering the attack on a systema clone device is made as mentioned above and it does not appear on the marketThe act of selling the recording medium of converting a certain Information Storage Division devicefor

examplerecording the data which should be enciphered essentially and should be recorded by a plaintext which made perform unjust record and was made as a result and containing the data recorded unjustly can be considered. In this caseif the device which recorded data on that recording medium unjustly can be specifiedit is possible by the above-mentioned method to distribute so that it may be eliminated from a system and new contents data may not be made to decode with that device.
[0018]This invention solves an above-mentioned problem.
The purpose records an own digital signature and public key certification with datawhen the Information Storage Division device records data on an information recording mediumWhen an information reproducing device reads dataafter checking the justification of the above-mentioned digital signature and a public key certificationby having composition which reads datait is providing the system which makes reproduction possible on condition that contents recording's is performed justly.

[0019]
[Means for Solving the Problem]In an information reproducing device with which the 1st side of this invention reproduces information from a recording mediumPerform verification processing of an enciphered content record subject's public key certification stored in said recording mediumand said contents recording subject's public key is acquired from a public key certification in which justification was checkedBased on an acquired this public keyverification processing of a contents recording subject's digital signature is performedand it is in an information reproducing device performing decoding processing of enciphered content on condition that the justification of a signature was checked as a result of this verification.
[0020]An information reproducing device of this invention sets like 1 operative conditionand said cipher-processing meansIt is characterized by being the composition of performing verification processing of a contents recording subject's digital signature generated considering contents of enciphered content stored in said recording medium as a candidate for a signatureand performing decoding processing of enciphered content as a result of this verification on condition that the justification of a signature was checked.
[0021]An information reproducing device of this invention sets like 1 operative conditionand said cipher-processing meansVerification processing of a contents recording subject's digital signature generated considering a title key set up corresponding to enciphered content stored in said recording medium as a candidate for a signature is performedIt is characterized by being the composition of performing decoding processing of enciphered content on condition that the justification of a signature was checked as a result of this verification.
[0022]An information reproducing device of this invention sets like 1 operative conditionand said information reproducing deviceHold a node key peculiar to each node which constitutes hierarchy key tree structure which used several different

information reproducing devices as a leafand a leaf key peculiar to each information reproducing deviceand said cipher-processing meansDecoding of validation key blocks (EKB) which consist of encryption processed data of a higher rank key by a low rank key on a path of a key tree based on a key built in said information reproducing device is performed. It has the composition which acquires data for decryption key generation required for decoding processing of code data stored in said recording medium.

[0023]An information reproducing device of this invention sets like 1 operative conditionand said data for decryption key generation is characterized by being a medium key peculiar to a common master key or a recording medium in two or more information reproducing devices.

[0024]In the Information Storage Division device with which the 2nd side of this invention records information to a recording mediumHave a cipher-processing means to perform encryption processing of contents stored in a recording mediumand this cipher-processing meansA digital signature of a record subject of said storing contents is generatedand it is in enciphered contenta digital signatureand the Information Storage Division device having the composition which performs processing which matches an enciphered content record subject's public key certificationand is stored in a recording medium.

[0025]The Information Storage Division device of this invention sets like 1 operative conditionsaid Information Storage Division device generates storing contentsa digital signatureand a management table that matched an address of a public key certificationand it has the composition which performs processing stored in said recording medium.

[0026]The Information Storage Division device of this invention sets like 1 operative conditionand said cipher-processing meansIt is characterized by being the composition of performing generation processing of a contents recording subject's digital signature by making applicable to a signature contents of enciphered content stored in said recording mediummatching a generated signature with storing contents and storing it.

[0027]The Information Storage Division device of this invention sets like 1 operative conditionand said cipher-processing meansIt is characterized by being the composition of performing generation processing of a contents recording subject's digital signature by making applicable to a signature a title key set up corresponding to enciphered content stored in said recording mediummatching a generated signature with storing contents and storing it.

[0028]The Information Storage Division device of this invention sets like 1 operative conditionand said Information Storage Division deviceHold a node key peculiar to each node which constitutes hierarchy key tree structure which used several different Information Storage Division devices as a leafand a leaf key peculiar to each Information Storage Division deviceand said cipher-processing meansDecoding of validation key blocks (EKB) which consist of encryption processed data of a higher rank key by a low rank key on a path of a key tree based on a key built in said Information Storage Division device is performed. It

has the composition which acquires data for cryptographic key generation required for data encryption processing stored in said recording medium.
[0029]The Information Storage Division device of this invention sets like 1 operative conditionand said data for cryptographic key generation is characterized by being a medium key peculiar to a common master key or a recording medium in two or more Information Storage Division devices.
[0030]In an information reproduction mode with which the 3rd side of this invention reproduces information from a recording mediumPublic key certification verification steps which perform verification processing of an enciphered content record subject's public key certification stored in said recording mediumSaid contents recording subject's public key is acquired from a public key certification in which justification was checkedSignature verification steps which perform verification processing of a contents recording subject's digital signature based on an acquired this public keyIt is in an information reproduction mode having a step which performs decoding processing of enciphered content on condition that the justification of a signature was checked as a result of this signature verification.
[0031]Said signature verification steps [ in / an information reproduction mode of this invention sets like 1 operative conditionand / said information reproduction mode ]A step which performs verification processing of a contents recording subject's digital signature generated considering contents of enciphered content stored in said recording medium as a candidate for a signature is includedAs a result of this verificationon condition that the justification of a signature was checkeddecoding processing of enciphered content is performed.
[0032]Said signature verification steps [ in / an information reproduction mode of this invention sets like 1 operative conditionand / said information reproduction mode ]A step which performs verification processing of a contents recording subject's digital signature generated considering a title key set up corresponding to enciphered content stored in said recording medium as a candidate for a signature is includedAs a result of this verificationon condition that the justification of a signature was checkeddecoding processing of enciphered content is performed.
[0033]An information reproduction mode of this invention sets like 1 operative conditionand said information reproduction modeBased on a node key peculiar to each node which constitutes hierarchy key tree structure which used several different information reproducing devices as a leafand a leaf key peculiar to each information reproducing deviceProcessing which acquires data for decryption key generation required for decoding processing of code data which performed decoding of validation key blocks (EKB) and was stored in said recording medium is performed.
[0034]In an Information Storage Division method that the 4th side of this invention records information to a recording mediumA cipher-processing step which performs encryption processing of contents stored in a recording mediumIt is in an Information Storage Division method having a step which generates a digital signature of a record subject of said storing contentsand enciphered contenta

digital signature and a step that matches an enciphered content record subject's public key certificationand is stored in a recording medium.
[0035]An Information Storage Division method of this invention sets like 1 operative conditionsaid Information Storage Division method generates further storing contentsa digital signatureand a management table that matched an address of a public key certificationand processing stored in said recording medium is performed.
[0036]An Information Storage Division method of this invention sets like 1 operative conditionand said Information Storage Division methodGeneration processing of a contents recording subject's digital signature is performed by making applicable to a signature contents of enciphered content stored in said recording mediumand a generated signature is matched with storing contents and stored.
[0037]An Information Storage Division method of this invention sets like 1 operative conditionand said Information Storage Division methodGeneration processing of a contents recording subject's digital signature is performed by making applicable to a signature a title key set up corresponding to enciphered content stored in said recording mediumand a generated signature is matched with storing contents and stored.
[0038]An Information Storage Division method of this invention sets like 1 operative conditionand said Information Storage Division methodFurthermoreDecoding of validation key blocks (EKB) is performed based on a node key peculiar to each node which constitutes hierarchy key tree structure which used as a leaf a different Information Storage Division device of plurality built in said Information Storage Division deviceand a leaf key peculiar to each Information Storage Division device. Processing which acquires data for cryptographic key generation required for data encryption processing stored in said recording medium is performed.
[0039]The 5th side of this invention is the information recording medium which stored enciphered contentand is in an information recording medium storing identification data of a record subject who recorded this enciphered contentsaid record subject's public key certificationand said record subject's digital signature.
[0040]An information recording medium of this invention set like 1 operative conditionand said information recording medium stored further storing contentsa digital signatureand a management table that matched an address of a public key certification.
[0041]The 6th side of this invention is the program storing medium which stored a computer program which makes information reproduction processing which reproduces information from a recording medium perform on computer systemsPublic key certification verification steps which perform verification processing of a public key certification of an enciphered content record subject by whom said computer program was stored in said recording mediumSaid contents recording subject's public key is acquired from a public key certification in which justification was checkedSignature verification steps which perform verification

processing of a contents recording subject's digital signature based on an acquired this public keyIt is in a program storing medium having a step which performs decoding processing of enciphered content on condition that the justification of a signature was checked as a result of this signature verification.
[0042]The 7th side of this invention is the program storing medium which stored a computer program which makes the Information Storage Division processing which records information to a recording medium perform on computer systemsA cipher-processing step which performs encryption processing of contents which store said computer program in a recording mediumIt is in a program storing medium having a step which generates a digital signature of a record subject of said storing contentsand enciphered contenta digital signature and a step that matches an enciphered content record subject's public key certificationand is stored in a recording medium.
[0043]
[Function]In this inventionwhen the Information Storage Division device recorded data on an information recording mediuman own digital signature and public key certification were recorded with data. Since he is trying to also certainly record with data proof which recorder recordedby this when recording informationSince it can specify which recorder recorded it even if the recording medium containing the data recorded unjustly circulatedexclusion from a system can be performed.
[0044]When an information reproducing device reads dataafter checking the justification of the above-mentioned digital signature and a public key certificationit had composition which reads data. By thisthe inaccurate recorder is delivering the powerless thing an attack which does not record a digital signature to inaccurate record data. That isit is because just playback equipment will not reproduce the data if there is no effective digital signature to the recorded data.
[0045]
[Embodiment of the Invention][System configuration] Drawing 1 is a block diagram showing one working example composition of the recording and reproducing device 100 which applied this invention. The recording and reproducing device 100Input-and-output I/F. 120 (Interface) MPEG (Moving.) Input-and-output I/F(Interface) 140 [ provided with the Picture Experts Group codec 130A/Dand D/A converter 141 ]the cipher-processing means 150ROM(Read Only Memory) 160CPU (Central.) Processing Unit170the memory 180and the recording-medium interface (I/F) 190 of the recording medium 200 -- it has the transport stream processing means (TS processing means) 300 furtherand these are mutually connected by bus 110.
[0046]Input-and-output I/F120 receives the digital signal on the bus 110and outputs it outside while it receives the digital signal which constitutes various contents supplied from the outsidesuch as a picturea soundand a programand outputs it on the bus 110. The MPEG codec 130 carries out MPEG encoding of the digital signal supplied from input-and-output I/F140and outputs it on the bus 110 while it carries out MPEG decoding of the data which is supplied via the bus 110 and by which MPEG coding was carried out and outputs it to input-and-output I/F140. Input-and-output I/F140 builds in A/D and D/A converter 141. It is

input-and-output I/F140 receiving the analog signal as contents supplied from the outsideand carrying out A/D (Analog Digital) conversion by A/D and D/A converter 141As a digital signalwhile outputting to the MPEG codec 130the digital signal from the MPEG codec 130 is outputted outside as an analog signal by carrying out D/A (Digital Analog) conversion by A/D and D/A converter 141.
[0047]For example the cipher-processing means 150 comprises LSI (Large Scale IntegratedCurcuit) of one chipenciphers or decodes the digital signal as contents supplied via the bus 110and has the composition outputted on the bus 110. Not only 1 chip LSI but the thing which the composition which combined various kinds of software or hardwares realizes is possible for the cipher-processing means 150. The latter part explains the composition as a processing means by a software configuration.
[0048]ROM160 has memorized the leaf key which is peculiar debye skiingand the node key which are two or more recording and reproducing devices or debye skiing shared in two or more groups for every recording and reproducing device for every group of two or more peculiar or recording and reproducing devicesfor example. The secret key of a public-key-encryption system peculiar to a recording and reproducing device and the public key of the public key certification and the further reliable center are memorized.
[0049]Herethe center (certificate authority) which a public key certification stores the certificate user'sfor exampleID of a recording and reproducing device and a userpublic key as shown in drawing 2and can trust other data as a message is the data which gave the digital signature. Verification processing of the digital signature of a center can be performed using the public key of an acquired center beforehandthe justification of a public key certification can be checkedand the stored public key can be taken out and used.
[0050]CPU170 is executing the program memorized by the memory 180and controls the MPEG codec 130 and cipher-processing means 150 grade. The memory 180 is nonvolatile memory and memorizes required data on the program which CPU170 executesand operation of CPU170for example. While the recording-medium interface 190 reads digital data from the recording medium 200 (reproducing) and outputs it on the bus 110 by driving the recording medium 200 in which record reproduction is possible for digital dataThe digital data supplied via the bus 110 is supplied to the recording medium 200and is made to record. It is good also as composition which memorizes a program to ROM160 and memorizes debye skiing etc. in the memory 180.
[0051]The recording medium 200 is a medium which can memorize digital datasuch as semiconductor memorysuch as optical discssuch as DVD and CDa magneto-optical disca magnetic diskmagnetic tapeor RAMfor example.
According to this embodimentsuppose that it is removable composition to the recording-medium interface 190.
Howeverthe recording medium 200 is good also as composition built in the recording and reproducing device 100.
[0052]Although the transport stream processing means (TS processing means)

300 is explained in detail using figures in the latter partFor examplethe transport packet corresponding to a specific program (contents) is taken out from the transport stream which two or more TV programs (contents) multiplexedData processing for storing the appearance timing information of the taken-out transport stream in the recording medium 200 with each packet and appearance timing-control processing at the time of the regeneration from the recording medium 200 are performed.

[0053]ATS (Arrival Time Stamp: mail arrival time stamp) as appearance timing information of each transport packet is set to the transport stream.

It is determined at the time of coding that this timing will not ruin T-STD (Transport stream System Target Decoder) which is the virtual decoder specified with MPEG 2 systemsand at the time of reproduction of a transport stream.

Appearance timing is controlled by ATS added to each transport packet.

The transport stream processing means (TS processing means) 300 performs these control. For examplein recording a transport packet on a recording mediumrecord as a source packet which packed the interval of each packetbut. By saving the appearance timing of each transport packet collectively at a recording mediumit becomes possible to control the output timing of each packet at the time of reproduction. The transport stream processing means (TS processing means) 300 adds and records ATS (ArrivalTime Stamp: mail arrival time stamp) showing the input timing of each transport packet at the time of Data Recording Sub-Division to the recording media 200such as DVD.

[0054]The data processed in the processing system of this invention is not restricted to the format data according to a transport stream. Thereforewhen performing processing about data other than a transport streamit is not necessarily necessary for TS processing means shown in drawing 1.

[0055][The Data Recording Sub-Division processing and data reproduction processing] Nextthe Data Recording Sub-Division processing and the data reproduction processing from a recording medium to the recording medium in the recording and reproducing device of drawing 1 are explained with reference to the flow chart of drawing 3 and drawing 4. When recording the contents of the digital signal from the outside on the recording medium 200recording processing according to the flow chart of drawing 3 (A) is performed. Namelythe contents (digital contents) of a digital signal. For examplevia IEEE(Institute of Electrical and Electronics Engineers) 1394 serial bus etc.If input-and-output I/F120 is suppliedin Step S11input-and-output I/F120 will receive the digital contents suppliedand will output them to TS processing means 300 or the cipher-processing means 150 via the bus 110.

[0056]When received data need transport stream processingtransport stream processing is performed in TS processing means 300. In Step S12TS processing means 300 generates the block data which added ATS to each transport packet which constitutes a transport streamand outputs it to the cipher-processing means 150 via the bus 110. This processing is explained still in detail in the latter part.

[0057]In Step S13the cipher-processing means 150 performs encryption processing to the digital contents which receivedand outputs the enciphered content obtained as a result to recording-medium I/F190 via the bus 110. Enciphered content is recorded on the recording medium 200 via recording-medium I/F190 (S14)and ends recording processing.
[0058]Between [ connected via the IEEE1394 serial bus ] devicesBy five companies which include Sony Corp. which is this Applicant as a standard for protecting digital contents when transmitting digital contents. Although 5CDTCP (Five Company Digital Transmission Content Protection) (suitably henceforth DTCP) is definedWhen the digital contents which are not free as for a copy are transmitted between devices in this DTCPIn [ attest mutually whether in advance of data communicationsthe transmitting side and a receiver can deal with the copy control information for controlling a copy correctlyand ] after that and the transmitting sideDigital contents are enciphered and transmitted and the enciphered digital contents (enciphered content) are decoded in a receiver.
[0059]In the data transmission and reception based on a standard to this DTCPIrput-and-output I/F120 of a data receiving side is Step S11it receives enciphered content via an IEEE1394 serial busdecodes the enciphered content to DTCP based on a standardand outputs it to the cipher-processing means 150 after that as contents of a plaintext.
[0060]The key which carries out a temporal change is generated and encryption of the digital contents by DTCP is performed using the key. The enciphered digital contents are transmitted in IEEE1394 serial bus tops including the key used for the encryptionand decode the enciphered digital contents in a receiver using the key contained there.
[0061]According to DTCPthe initial value of a key and the flag showing the changing timing of a key used for encryption of digital contents are correctly included in enciphered content. And at a receiverby changing too the initial value of the key contained in the enciphered content in the timing of the flag contained in the enciphered contentthe key used for encryption is generated and enciphered content is decoded. Howeverif the key for performing the decoding to enciphered content is containedeven if it will think that it is equivalentin order not to interferebelowit shall think such here. In the Web page specified by URL (Uniform Resource Locator) of http://www.dtcp.com about DTCP herefor exampleAcquisition of an informational version (Informational Version) is possible.
[0062]Nextthe contents of the analog signal from the outside are explained about the processing in the case of recording on the recording medium 200 according to the flow chart of drawing 3 (B). When the contents (analog content) of an analog signal are supplied to input-and-output I/F140input-and-output I/F140In Step S21the analog content is receivedan A/D conversion is carried out by A/D and D/A converter 141 which are followed and built in Step S22and it is considered as the contents (digital contents) of a digital signal.
[0063]These digital contents are supplied to the MPEG codec 130and in Step S23coding processing by MPEG encodingi.e.MPEG compressionis performedand

they are supplied to the cipher-processing means 150 via the bus 110.
[0064]Hereafterin Step S24S25and S26processing in Step S12 of drawing 3 (A)S13and S14 and same processing are performed. That isif requiredATS addition to the transport packet by TS processing means 300 and encryption processing in the cipher-processing means 150 will be performedthe enciphered content obtained as a result is recorded on the recording medium 200and recording processing is ended.
[0065]Nextthe contents recorded on the recording medium 200 are reproducedand the processing outputted as digital contents or analog content is explained according to the flow of drawing 4. Processing outputted outside as digital contents is performed as regeneration according to the flow chart of drawing 4 (A). That isfirstin Step S31the enciphered content recorded on the recording medium 200 is read by recording-medium I/F190and it is outputted to the cipher-processing means 150 via the bus 110.
[0066]In the cipher-processing means 150decoding processing of the enciphered content supplied from recording-medium I/F190 is carried out in Step S32and when data is a transport streamDecode data is outputted to TS processing means 300 via the bus 110and when TS processing is unnecessaryinput-and-output I/F120 s supplied.
[0067]In Step S43TS processing means 300 judges output timing from ATS of each transport packet which constitutes a transport streamperforms control according to ATSand supplies it to input-and-output I/F120 via the bus 110. Input-and-output I/F120 outputs the digital contents from TS processing means 300 outsideand ends regeneration. The decoding processing of the digital contents in processing of TS processing means 300 and the cipher-processing means 150 is mentioned later.
[0068]Data is supplied to input-and-output I/F120and in Step S34input-and-output I/F120 outputs digital contents outsideand ends regeneration.
[0069]Input-and-output I/F120 is Step S34based on the standard of DTCPwhen outputting digital contents via an IEEE1394 serial busas mentioned aboveattests mutually between a partner's devicesand enciphers and transmits digital contents after that.
[0070]When reproducing the contents recorded on the recording medium 200 and outputting outside as analog contentregeneration according to the flow chart of drawing 4 (B) is performed.
[0071]Namelyin Step S41S42and S43the respectively same processing as the case in Step S31 of drawing 4 (A)S32and S33 is performedand by thisThe decoded digital contents which were obtained in the cipher-processing means 150 are supplied to the MPEG codec 130 via the bus 110.
[0072]In the MPEG codec 130in Step S44MPEG decodingi.e.elongation processingis executed and digital contents are supplied to input-and-output I/F140. In Step S44D/A conversion (S45) of the digital contents by which MPEG decoding was carried out by the MPEG codec 130 is carried out by A/D and D/A converter 141 to build inand input-and-output I/F140 makes them analog content.

And it progresses to Step S46and input-and-output I/F140 outputs the analog content outsideand ends regeneration.
[0073][Transport stream] Nextthe data format on the recording medium in the case of processing transport stream data is explained using drawing 5. The minimum unit of reading and writing of the data on a recording medium is called by the name of the block (block). 1 block has 192*X (X) byte's (for exampleX= 32) size.
[0074]For exampleATS is added to TS (transport stream) packet (188 bytes) of MPEG 2and as 192 bytesX of them are collected and it is considered as 1-block data. ATS is data in which 24 thru/or 32-bit mail arrival time is shownand is the abbreviation for Arrival Time Stamp (mail arrival time stamp). ATS is constituted as data with the random nature according to the mail arrival time of each packet. X individual record of the TS (transport stream) packet which added ATS to one block (sector) of a recording medium is carried out. In the composition of this inventionthe block key which enciphers the data of the block (sector) using ATS added to the 1st TS packet of each block which constitutes a transport stream is generated.
[0075]By generating the block key for encryption using ATS with random naturea different inherent key for every block is generated. Encryption processing for every block is performed using the generated block inherent key. By having composition which generates a block key using ATSthe field on the recording medium for storing the enciphering key for every block becomes unnecessaryand a main data area becomes usable effectively. It becomes unnecessary to access any data other than a main data division at the time of record of dataand reproductionand processing becomes efficient.
[0076]Block seed (Block Seed) shown in drawing 5 is the additional information containing ATS. The composition which copy limit information (CCI:Copy Control Information) also adds as further shown not only in ATS but in the figure middle is possible for block seed. In this caseit can have composition which generates a block key using ATS and CCI.
[0077]In the composition of this inventionwhen it stores data on recording mediasuch as DVDthe data of most contents is encipheredbut. As shown in the bottom of drawing 5m (for examplem= 8 or 16) byte of the head of a block is recorded with a plaintext (Unencrypted data)without being encipheredand the remaining data (m+1 byte or subsequent ones) is enciphered. This is for restrictions to occur in cipher-processing data length (Encrypted data)since cipher processing is processing as an 8-byte unit. If cipher processing can carry out for example not per 8-byte unit but per byteall portions other than block seed may be enciphered as m= 4.
[0078][Processing in TS processing means] Herethe function of ATS is explained in detail. ATS is a mail arrival time stamp added since the appearance timing of each transport packet in an input transport stream is saved as explained also in advance.
[0079]Namelywhen one or some TV programs (contents) are taken out out of the

transport stream which two or more TV programs (contents) multiplexedfor exampleThe transport packet which constitutes the taken-out transport stream appears at an irregular interval (refer to drawing 7 (a)). A transport stream has a meaning important for the appearance timing of each transport packetIt is determined at the time of coding that this timing will not ruin T-STD (Transport stream System Target Decoder) which is the virtual decoder specified with MPEG 2 systems (ISO/IEC 13818-1).

[0080]Appearance timing is controlled by ATS added to each transport packet at the time of reproduction of a transport stream. Thereforein recording a transport packet on a recording medium. When it is necessary to save the input timing of a transport packet and a transport packet is recorded on recording mediasuch as DVDATS showing the input timing of each transport packet is added and recorded.

[0081]The block diagram explaining the processing which performs the transport stream inputted via a digital interface in TS processing means 300 when recording on the storage medium which are recording mediasuch as DVDis shown in drawing 6. From the terminal 600a transport stream is inputted as digital datasuch as digital broadcasting. In drawing 1a transport stream is inputted from the terminal 600 via input-and-output I/F140 and the MPEG codec 130 via input-and-output I/F120.

[0082]A transport stream is inputted into the bit stream purser (parser) 602. The bit stream purser 602 detects an PCR (Program Clock Reference) packet out of an input transport stream. Herean PCR packet is a packet by which PCR specified with MPEG 2 systems is coded. The PCR packet is coded with the time interval of less than 100 msec. PCR expresses with the accuracy of 27 MHz the time when a transport packet reaches a receiver.

[0083]And PCR of a transport stream is made to carry out lock (Lock) of the 27 MHz clocks which a record reproducer has in 27MHzPLL603. The time stamp generation circuit 604 generates the time stamp based on the counted value of the clock of 27 MHz clocks. And the block seed (Block seed) additional circuit 605 is added to the transport packet by setting a time stamp in case the 1st byte of a transport packet is inputted into the smoothing buffer 606 to ATS.

[0084]The transport packet to which ATS was addedIt passes along the smoothing buffer 606and after cipher processing which it is outputted to the cipher-processing means 150and is explained in the latter part from the terminal 607 is performedit is recorded on the recording medium 200 which is a storage medium via recording-medium I/F210 (drawing 1).

[0085]Drawing 7 shows the example of processing in case an input transport stream is recorded on a recording medium. Drawing 7 (a) shows the input of the transport packet which constitutes a certain specific program (contents). A horizontal axis is a time-axis which shows the time on a stream here. In this examplethe input of a transport packet appears to irregular timingas shown in drawing 7 (a).

[0086]Drawing 7 (b) shows the output of the block seed (Block Seed) additional circuit 605. The block seed (Block Seed) additional circuit 605 adds the block seed

(Block Seed) containing ATS which shows the time on the stream of the packet for every transport packetand outputs a source packet. Drawing 7 (c) shows the source packet recorded on the recording medium. As shown in drawing 7 (c)a source packet packs an interval and is recorded on a recording medium. Thusthe record section of a recording medium can be effectively used by packing and recording an interval.

[0087]Drawing 8 shows the processing constitution block diagram of TS processing means 300 in the case of reproducing the transport stream recorded on the recording medium 200. The transport packet with ATS decoded in a cipher-processing means to explain in the latter part is inputted into the block seed (Block seed) separation circuits 801and ATS and a transport packet are separated from the terminal 800. The timing generating circuit 804 calculates the time based on the clock counter value of 27 MHz clocks 805 which a regenerator has.

[0088]Very first ATS is set to the timing generating circuit 804 as an initial value at the time of a reproductive start. The comparator 803 compares the present time inputted from ATS and the timing generating circuit 804. And when time for the timing generating circuit 804 to occur and ATS become equalthe output controlling circuit 802 outputs the transport packet to the MPEG codec 130 or digital-input/output I/F120.

[0089]Drawing 9 carries out MPEG encoding of the input AV signal in the MPEG codec 130 of the record reproducer 100and shows the composition which codes a transport stream in TS processing means 300 further. Thereforedrawing 9 is a block diagram showing both the processing constitution of the MPEG codec 130 and TS processing means 300 in drawing 1 collectively. The video signal is inputted from the terminal 901 and it is inputted into MPEG video encoder 902.

[0090]MPEG video encoder 902 codes an input video signal to an MPEG video streamand outputs it to the buffer video stream buffer 903. MPEG video encoder 902 outputs the access unit information about an MPEG video stream to the multiplexing scheduler 908. The access unit of a video stream is a picture and access unit information is a picture type of each picturean encoding bit amountand a decoding time stamp. Herea picture type is the information on I/P/B picture (picture). A decoding time stamp is information specified with MPEG 2 systems.

[0091]The audio signal is inputted from the terminal 904 and it is inputted into MPEG audio encoder 905. MPEG audio encoder 905 codes an input audio signal to an MPEG audio streamand outputs it to the buffer 906. MPEG audio encoder 905 outputs the access unit information about an MPEG audio stream to the multiplexing scheduler 908. The access unit of an audio stream is an audio frameand access unit information is an encoding bit amount of each audio frameand a decoding time stamp.

[0092]The access unit information of video and an audio is inputted into the multiplexing scheduler 908. The multiplexing scheduler 908 controls the method of coding a video stream and an audio stream to a transport packet based on access unit information. As the multiplexing scheduler 908 has a clock which generates the reference time of 27-MHz accuracy in an inside and fills T-STD which is the

virtual decoder model specified by MPEG 2it determines the packet encoding control information of a transport packet. Packet encoding control information is the kind of stream and the length of a stream which are packet-ized.
[0093]When packet encoding control information is a video packetit is on the a sidethe video data of payload-data length directed by packet encoding control information is read from the video stream buffer 903and the switch 976 is inputted into the transport packet coding equipment 909.
[0094]When packet encoding control information is an audio packetit is on the b sidethe audio information of payload-data length directed from the audio stream buffer 906 is readand the switch 976 is inputted into the transport packet coding equipment 909.
[0095]When packet encoding control information is an PCR packetthe transport packet coding equipment 909 incorporates PCR inputted from the multiplexing scheduler 908and outputs an PCR packet. Nothing is inputted into the transport packet coding equipment 909 when directing that packet encoding control information does not code a packet.
[0096]The transport packet coding equipment 909 does not output a transport packetwhen directing that packet encoding control information does not code a packet. When othera transport packet is generated and outputted based on packet encodir g control information. Thereforethe transport packet coding equipment 909 outputs a transport packet intermittently. The arrival (Arrival) time stamp (time stamp) calculating means 910 calculates ATS which shows the time when the 1st byte of a transport packet reaches a receiver based on PCR inputted from the multiplexing scheduler 908.
[0097]Since PCR inputted from the multiplexing scheduler 908 shows the arrival time to the 10th byte of receiver of the transport packet specified by MPEG 2the value of ATS serves as time when the byte 10 bytes before the time of PCR arrives.
[0098]The block seed (Block Seed) additional circuit 911 adds ATS to the transport packet outputted from the transport packet coding equipment 909. The transport packet with ATS outputted from the block seed (Block seed) additional circuit 911It passes along the smoothing buffer 912a cipher-processing means 150 HE input is carried outand it is stored in the recording medium 200 which is a storage medium after cipher processing explained in the latter part is performed.
[0099]Before being enciphered by the cipher-processing means 150the transport packet with ATS stored in the recording medium 200 is inputted where an interval is packedas shown in drawing 7 (c)and it is stored in the recording medium 200 after that. Even if a transport packet packs an interval and is recordedthe input time to the receiver of the transport packet is controllable by referring to ATS.
[0100]By the waythe size of ATS was not necessarily decided as 32 bitsand 24 bits thru/or 31 bits of it may be sufficient. The cycle around which the time counter of ATS goes becomes longso that the bit length of ATS is long. For examplewhen ATS is a binary counter of 27-MHz accuracytime for ATS of 24-bit length to go around is about 0.6 second. This time interval is size sufficient in a

general transport stream. It is because the packet interval of the transport stream is decided to be a maximum of 0.1 second by regulation of MPEG 2.
Howeversufficient margin is seen and it is good as for more than 24-bit in ATS.
[0101]Thuswhen bit length of ATS is made into various lengthsome composition is attained as composition of the block seed who is attached data of block data.
Block seed's example of composition is shown in drawing 10. Example 1 of drawing 10 is an example which uses ATS by 32 bits. Example 2 of drawing 10 is an example which makes ATS 30 bits and uses copy control information (CCI) by 2 bits. Copy control information is information showing the state of copy-of-data control where it was added.
SCMS:Serial Copy Management System and CGMS:Copy Generation Management System are famous.
Copy free (Copy Free) which shows that the copy is permitted without restriction in such copy control information as for the data in which the information was addedInformationincluding the copy prohibition (Copy Prohibited) etc. which do not accept the one-generation copy permission (One Generation Copy Allowed) which permits the copy of only one generationand a copycan be expressed.
[0102]Example 3 shown in drawing 10 is an example which makes ATS 24 bitsuses 2 bits of CCI(s)and uses 6 bits of information of further others. As other informationwhen the analog output of this data is carried outfor exampleit is possible to use various informationincluding information etc.which shows ON and OFF (On/Off) of the macro vision (Macrovision) which is a copy control mechanism of an analog video data.
[0103][Tree (Thurs.) structure as key distribution composition] Nextthe composition which distributes the key which needs it when the recording and reproducing device shown in drawing 1 reproduces data from record or a recording medium to a recording mediumfor examplea medium keyto each apparatus is explained. Drawing 11 is a figure showing the distribution composition of the key of the recording and reproducing device in the recording system which used this method. The numbers 0-15 shown in the bottom of drawing 11 are each recording and reproducing devices. That iseach leaf (leaf: leaf) of the tree (tree) structure shown in drawing 11 is equivalent to each recording and reproducing device.
[0104]Each devices 0-15 store in person the key (node key) assigned to the node of a to [ from its own leaf in the initial tree defined beforehand / a route ]and the leaf key of each leaf at the time of manufacture (at the time of shipment). K0000-K1111 which are shown in the bottom of drawing 11 are the leaf key assigned to each devices 0-15respectivelyand let key:KR-K111 indicated in the 2nd paragraph (node) from the bottom be a node key from KR of the highest rung.
[0105]In the tree composition shown in drawing 11the device 0 owns the leaf key K0000node key:K000 and K00K0and KR. The device 5K0101K010K01K0and KR are owned. The device 15 owns K1111K111K11K1and KR. Although 16 devices of 0-15 are indicated to the tree of drawing 11 and the tree structure is also shown as symmetrical composition which was able to take balance of 4 stage constitutionit is possible to have number-of-stages composition which much more devices are

constituted in a treeand is different in each part of a tree.
[0106]The record reproducer various type which uses various recording mediafor exampleDVDCDMDa memory stick (trademark)etc. is contained in each record reproducer contained in the tree structure of drawing 11. It is assumed that various application services live together. The key distribution composition shown in drawing 11 after such a different device and different application constitute [ coexistence ] is applied.
[0107]Ir the system by which these various devices and application live togetherthe portion 012and 3 enclosed with the dotted line of drawing 11i.e.devicesis set up as one group using the same recording medium. For examplethe device contained in the group enclosed with this dotted line is receivedIt collectsand common contents are enciphered and processing in which send the master key which is sent from a provider or is used in commonor encipher to a provider or a settlement-of-accounts organization tooand the payment data of a content rate is outputted to it from each device is performed. Organizations which perform data transmission and reception with each devicesuch as a content provider or a settlement processing organizationperform the portion enclosed with the dotted line of drawing 11i.e.the processing which bundle up the devices 012and 3 as one groupand sends data. Two or more such groups exist in the tree of drawing 11.
[0108]A node key and a leaf key are good also as composition managed for every group with the provider who may generalize and manage by one certain lock management centerand performs various data transmission and reception to each groupa settlement-of-accounts organizationetc. As for these node keys and a leaf keyin disclosure of a keyetc.an update process is performedand a lock management centera providera settlement-of-accounts organizationetc. perform this update process.
[0109]In this tree structurethe three devices 012and 3 contained in one group hold the key K00 common as a node keyK0and KR so that clearly from drawing 11. By using this node key share compositionit becomes possible to provide only the devices 012and 3 with a common master keyfor example. For exampleif node key K00 the very thing held in common is set up as a master keysetting out of a master key only with the common devices 012and 3 is possiblewithout performing new key sending. If the value Enc (K00Kmaster) which enciphered the new master key Kmaster by the node key K00 is stored in a recording medium via a network and distributed to the devices 012and 3Only the devices 012and 3 become possible [ solving the code Enc (K00 Kmaster) using the share node key K00 held in each deviceand obtaining master key:Kmaster ]. It is shown that Enc (KaKb) is the data which enciphered Kb by Ka.
[0110]When it is revealed in t at a certain time that key:K0011 which the device 3 ownsK001K00K0and KR were analyzed by the aggressor (hacker)and it was exposed of KRAfter itin order to protect the data transmitted and received by a system (group of the devices 012and 3)it is necessary to separate the device 3 from a system. for that purpose -- a node key -- : -- K -- 001 -- K -- 00 -- K -

- zero -- KR -- respectively -- being new -- a key -- K -- (-- t --) -- 001 -- K -- (-- t --) -- 00 -- K -- (-- t --) -- zero -- K -- (-- t --) -- R -- updating -- a device -- zero -- one -- two -- the -- updating -- a key -- it is necessary to tell . Hereit is shown that K(t) aaa is an updating key of generation (Generation):t of the key Kaaa.

[0111]Distribution processing of an updating key is explained. The renewal of a key the table constituted by the block data called the validation key blocks (EKB:Enabling Key Block) shown in drawing 12 (A)for example For examplea networkOr it performs by storing in a recording medium and supplying the devices 01and 2.

[0112]It is constituted as block data which has a data configuration which can update only the required device of renewal of a node key in the validation key blocks (EKB) shown in drawing 12 (A). In the devices 01and 2 in the tree structure shown in drawing 11the example of drawing 12 is the block data formed for the purpose of distributing the generation's t updating node key. drawing 11 -- from -- being clear -- as -- a device -- zero -- a device -- one -- updating -- a node key -- ****** -- K -- (-- t --) -- 00 -- K -- (-- t --) -- zero -- K -- (-- t --) -- R -- required -- a device -- two -- updating -- a node key -- ****** -- K -- (-- t --) -- 001 -- K -- (-- t --) -- 00 -- K -- (-- t --) -- zero -- K -- (-- t --) -- R -- being required .

[0113]As shown in EKB of drawing 12 (A)two or more cryptographic keys are contained in EKB. The cryptographic key of the bottom is Enc (K0010K(t)001). this -- a device -- two -- having -- a leaf key -- K -- 0010 -- enciphering -- having had -- updating -- a node key -- K -- (-- t --) -- 001 -- it is -- a device -- two -- self -- having -- a leaf key -- this -- a cryptographic key -- decoding -- K -- (-- t --) -- 001 -- it can obtain . using K(t)001 obtained by decodingdecoding of the 2nd step of cryptographic key Enc (K -- (-- t --) -- 001 -- K -- (-- t --) -- 00) is attained from under drawing 12 (A)and updating node key K(t)00 can be obtained. belowone by onethe 2nd step of cryptographic key Enc (K -- (-- t --) -- 00 -- K -- (-- t --) -- 0) is decoded from on drawing 12 (A)the 1st step of cryptographic key Enc (K(t) 0 and K (t) R) is decoded from on updating node key K(t)0 and drawing 12 (A)and K(t) R is obtained. on the other hand -- a device -- zero -- one -- a node key -- K -- 000 -- updating -- an object -- containing -- not having -- updating -- a node key -- ****** -- being required -- a thing -- K -- (-- t --) -- 00 -- K -- (-- t --) -- zero -- K -- (-- t --) -- R -- it is . The devices 0 and 1 decode the 3rd step of cryptographic key Enc (K000K(t)00) from on drawing 12 (A)and acquire K(t)00hereafterthe 2nd step of cryptographic key Enc (K -- (-- t --) -- 00 -- K -- (-- t --) -- 0) is decoded from on drawing 12 (A)the 1st step of cryptographic key Enc (K(t) 0 and K (t) R) is decoded from on updating node key K(t)0 and drawing 12 (A)and K(t) R is obtained. Thusthe devices 01and 2 can obtain updated key K(t) R. The index of drawing 12 (A) shows the actual address of the node key and leaf key which are used as a decryption key.

[0114]The node key of the upper stage of the tree structure shown in drawing 11 : when renewal of K(t) 0 and K (t) R is unnecessary and the update process of only

the node key K00 is requiredBy using the validation key blocks (EKB:Enabling Key Block) of drawing 12 (B)updating node key K(t)00 can be distributed to the devices 01and 2.

[0115]EKB shown in drawing 12 (B) is available when distributing a medium key peculiar to the new master key sharedfor example in a specific groupor a recording medium. As an examplethe recording medium with the devices 012and 3 in the group who shows by a dotted line is used for drawing 11and suppose that new common master key K(t) master is required. this -- the time -- a device -- zero -- one -- two -- three -- being common -- a node key -- K -- 00 -- having updated -- K -- (-- t --) -- 00 -- using -- being new -- being common -- updating -- a master key -- : -- K -- (-- t --) -- master -- having enciphered -- data -- Enc (K (t)K(t) master) -- drawing 12 -- (-- B --) -- being shown -- EKB -- distributing . By this distributionthe distribution as data of the device 4 etc. which is not decoded in other groups' apparatus is attained. The same may be said of a medium key.

[0116]That isif the devices 01and 2 decode the above-mentioned cryptogram using K(t)00 which processed and obtained EKBit will become possible to obtain master key:K(t) master in t timeand medium key:K(t) media.

[0117][Acquisition of the medium key which uses EKB] as an example of processing which obtains medium key K(t) media in t time proposed to drawing 13 by Japanese Patent Application No. 2000-105328 which is the patent application of these people's pointK (t) Processing of the device 2 which received EKB shown in the data Enc (K(t) 00 and K (t) media) which enciphered new common medium key K(t) media using 00and drawing 12 (B) via the recording medium is shown.

[0118]As shown in drawing 11suppose that four devices of the devices 012and 3 surrounded by the dotted line are contained in a certain recording and reproducing system. When are RIBOKU the device 3 and using the medium key assigned for every recording mediumdrawing 13The processing at the time of asking for a medium key required in order that a recording and reproducing device (device 2) may encipher or decode the contents on a recording medium using the debye skiing which EKB (EnablingKey Block) stored in the recording medium and a recording and reproducing device memorize is expressed.

[0119]The leaf key K_0010 assigned only to itself and the node key (respectively K_001K_00K_0K_R) of each nodes 00100and 0R from it to a wooden route are safely stored in the memory of the device 2. The device 2 calculates node key K(t)_001 of the node 001 by index (index) decoding the cryptogram of 0010 among EKB(s) stored in the recording medium of drawing 13 by the leaf key K_0010 which he hasNextit needs to calculate medium key K(t)_media using it by decoding the cryptogram of 001and index (index) calculating node key K(t)_00 of the node 00using it finallyand decoding a cryptogram. These calculation times increase in proportion to the depth to the node which enciphers a medium key from a leaf becoming deep. That isin the big system by which many recording and reproducing devices existmany calculations are needed. Thusthe data encryption processing and the decoding processing mode using the medium key calculated and acquired

are explained hereafter.
[0120][Contents recording processing using a medium key] According to the processing block figure of drawing 14an example of encryption processing of the data which the cipher-processing means 150 performsand the recording processing to a recording medium is explained.
[0121]The recording and reproducing device 100 shown in drawing 14 acquires a medium key by calculation processing based on EKB which self mentioned above.
[0122]Nextit is inspected whether as for the recording and reproducing device 100disk ID (Disc ID) as identification information is already recorded on the recording medium 200 which is an optical disc. If recordeddisk ID (Disc ID) is readand if not recordedfor exampleit was set at random or beforehand in the cipher-processing means 150disk ID (Disc ID) will be generated by methodssuch as a random number generationand it will record on a disk. The thing with one stored in read in area etc. since it is good is also possible for disk ID (Disc ID) on the disk.
[0123]A medium key and disk ID are used for the record reproducer 100 nextand it generates a disk inherent key (Disc Unique Key). As a concrete generation method of a disk inherent key (Disc Unique Key)The method of Example 1 using the result obtained by inputting a medium key and disk ID (Disc ID) into the hash function using a block cipher function as shown in drawing 15To hash function SHA-1 defined by FIPS 180-1. The data generated by the bit connection to a medium key and disk ID (Disc ID) is inputtedand the method of Example 2 which uses only required data length as a disk inherent key (Disc Unique Key) from the output of 160 bits can be applied.
[0124]Nextfor exampletitle key (Title Key) which is an inherent key for every record was defined at random or beforehand in the cipher-processing means 150 (refer to drawing 1)it generates by methodssuch as a random number generationand records on the disk 200.
[0125]Nextthe combination of title key (Title Key) to a disk inherent key (Disc Unique Key) and a title inherent key (Title Unique Key) are generated.
[0126]The concrete method of this title inherent key (Title Unique Key) generationThe method of Example 1 using the result obtained by enciphering a title key by using a disk inherent key as a key using a block cipher function as shown in drawing 16To hash function SHA-1 defined by FIPS 180-1. The data generated by the bit connection to a medium key and disk ID (Disc ID) is inputtedand the method of Example 2 which uses only required data length as a title inherent key (Title Unique Key) from the output of 160 bits can be applied.
[0127]In the above-mentioned explanationa disk inherent key (Disc Unique Key) is generated from a medium key and disk ID (Disc ID)Although he is trying to generate a title inherent key (Title Unique Key) from this and the title key (Title Key)respectivelya title inherent key (Title Unique Key) being directly generated from a medium keydisk ID (Disc ID)and the title key (Title Key)using a disk inherent key (Disc Unique Key) as unnecessaryandA key equivalent to a title inherent key (Title Unique Key) may be generated from a medium key (Master Key)

and disk ID (Disc ID)without using the title key (Title Key).
[0128]Subsequent processing is explained using drawing 14. The block seed (Block Seed) who the 1-4th byte of the head of the block data inputted as encrypted data is separatedand is outputtedFrom the title inherent key (Title Unique Key) generated previouslythe block key (BlockKey) which is a key which enciphers the data of the block is generated.
[0129]The example of the generation method of block key (Block Key) is shown in drawing 17. By drawing 17each shows two examples which generate the 64-bit block key (Block Key) from 32 bits block seed (Block Seed) and a 64-bit title inherent key (Title Unique Key).
[0130]64 bits of key length and the code function whose input and output are 64 bitsrespectively are being used for Example 1 shown in the upper row. A title inherent key (Title Unique Key) is used as the key of this code functionand the result which inputted the value which connected the constant (constant) of 32 bits with block seed (Block Seed)and was enciphered is made into the block key (Block Key).
[0131]Example 2 is an example which used hash function SHA-of FIPS 180-1 1. The value which connected the block seed (Block Seed) with the title inherent key (Title Unique Key) is inputted into SHA-1What was contracted to 64 bitssuch as 64 bits of low ranks accepting the output of 160 bitsand using itfor exampleis made into the block key (Block Key).
[0132]Although the example which generates a disk inherent key (Disc Unique key)a title inherent key (Title Unique Key)and the block key (Block Key) aboverespectively was explainedFor examplewithout performing generation of a disk inherent key (Disc Unique Key) and a title inherent key (Title Unique Key)The block key (Block Key) may be generated using a medium keydisk ID (Disc ID)title key (Title Key)and the block seed (Block Seed) for every block.
[0133]Generation of a block key will encipher block data using the generated block key (Block Key). As shown in the lower berth of drawing 14it dissociates (selector 1608)and the 1st - m byte (for examplem= 8 bytes) of the head of block data including the block seed (Block Seed) do not consider it as the candidate for encryptionbut enciphers from the m+1st byte to final data. In m byte who is not encipheredthe 1-4th byte as BURROKU seed is also contained. The block data after the m+1st byte separated by the selector is enciphered according to the encryption algorithm beforehand set as the cipher-processing means 150. As an encryption algorithmDES (Data Encryption Standard) specifiedfor example by FIPS 46-2 can be used.
[0134]Contents are block unitsand encryption is given by the above processing with the block key generated based on the medium key by which generation management was carried outblock seedetc.and they are stored in a recording medium by it.
[0135]Nextto the recorded enciphered content dataa recording and reproducing device calculates a digital signature using the secret key (signature generating key) of a public-key-encryption system assigned to selfand records this on a

recording medium with an own public key certification and contents data. As a generation method of a digital signatureEC-DSA (Elliptic Curve Digital Signature Algorithm) under standard establishment can be used by IEEE P1363for example. The flow chart explaining the outline of the recording processing of contents is shown in drawing 18.

[0136]Firsta recording and reproducing device performs encryption processing of recording object contents in Step S101. Contents encryption is performed as encryption processing of the block data using a block keyas explained using drawing 14.

[0137]In Step S102a recording and reproducing device calculates the digital signature to enciphered content using the secret key (signature generating key) of a public-key-encryption system assigned to self. As a generation method of a digital signatureEC-DSA (Elliptic Curve Digital Signature Algorithm) under standard establishment is applicable by IEEE P1363for example.

[0138]Nextin Step S103a recording and reproducing device matches with record contents the digital signature and public key certification which were generatedand records them on a recording mediumand recording processing (S102) to the recording medium of encryption data is performed in Step S104.

[0139]The detailed process flow in the case of performing a digital signature to enciphered content and performing record is shown in drawing 19.

[0140]In Step S201a recording and reproducing device acquires a medium key by the above-mentioned EKB processing (refer to drawing 13).

[0141]In S202it is inspected whether disk ID (Disc ID) as identification information is already recorded on the recording medium. If are recordedand this disk ID is read and it is not recorded by S203by S204disk ID is generated by the method defined at random or beforehandand it records on a disk. Nextin S205a disk inherent key is generated using a medium key and disk ID. It asks to have explained the disk inherent key previously by applying the method of using hash function SHA-1 defined by FIPS 180-1the method (refer to drawing 15) of using the hash function based on a block cipheretc.

[0142]Nextit progresses to S206and the title key (Title Key) as a peculiar key for the one record of every is generatedand the generated title key is recorded on a disk (recording medium). Nextby S207a title inherent key is generated from the above-mentioned disk inherent key and a title key (refer to drawing 16).

[0143]A recording and reproducing device receives S208 the encrypted data of the contents data which should be recorded in the form of a TS packet. By S209TS processing means 300 adds ATS which is the time information which received each TS packet. Or the value which combined the copy control information CCI and ATS and the information of further others is added. Nextit is judged whether the TS packet which added ATS was received one by one by S2101 block is formedfor examplethe identification data in which whether it having amounted to X= 32 and the end of a packet are shown was received. When one of conditions is satisfiedit progresses to Step S211and the packet to X individual or the end of a packet is put in orderand 1-block block data is formed.

[0144]Nextthe cipher-processing means 150 is S212 and generates the block key which is a key which enciphers the data of the block from 32 bits (block seed containing ATS) of the head of block dataand the title inherent key generated by S207 (refer to drawing 17).
[0145]In S213the block data formed by S211 using the block key is enciphered. As explained also in advanceit is the m+1st byte to final data of block data that it is the target of encryption. DES (Data Encryption Standard) as which an encryption algorithm is specifiedfor example by FIPS 46-2 is applied.
[0146]By S214it judges whether a recording block is the 1st blockand when it is the 1st blockin S215a digital signature is generated by using block data as digital signature object dataand it records on a recording medium with a public key certification. The generation processing of a digital signature applies EC-DSA (Elliptic Curve Digital Signature Algorithm) under standard establishment for exampleby IEEE P1363.
[0147]By S216the enciphered block data is recorded on a recording medium. By S217it is judged whether all the data was recorded. If all the data is recordedrecording processing is ended and all the data is not recordedit will return to S208 and processing of the remaining data will be performed.
[0148]Contents will be enciphered by the above processingit will be recorded on a recording mediumand the digital signature to the block data of enciphered content and a public key certification will be further recorded on a recording medium.
[0149]The contents stored in a recording mediuma title keya DEJITASHIRU signaturea public key certificationand other contents associated data are recorded with composition identifiable in each correspondence. For exampleit can match by recording on a recording medium by using management data as a table. The example of a table format in the case of recording the address information of the associated data about record contents as a table is shown in drawing 20.
[0150]As shown in drawing 20each contents with contents associated data. It is managed as a filethe address of contents datathe address of a title keythe address of a digital signaturethe address of a public key certificationand the other tables recorded about file information are generatedand it is stored in a recording medium.
[0151]Nextwhen recording enciphered content on a recording mediumthe processing which does not perform a signature to enciphered contentbut performs a digital signature to the title key generated corresponding to contentsand performs contents recording is explained using the flow of drawing 21.
[0152]In Step S301a recording and reproducing device acquires a medium key by the above-mentioned EKB processing (refer to drawing 13).
[0153]In S302it is inspected whether disk ID (Disc ID) as identification information is already recorded on the recording medium. If are recordedand this disk ID is read and it is not recorded by S303by S304disk ID is generated by the method defined at random or beforehandand it records on a disk. Nextin S305a disk inherent key is generated using a medium key and disk ID. It asks to have explained the disk inherent key previously by applying the method of using hash

function SHA-1 defined by FIPS 180-1the method (refer to drawing 15) of using the hash function based on a block cipheretc.
[0154]Nextit progresses to S306and the title key (Title Key) as a peculiar key for the one record of every is generatedand the digital signature to the generated title key is performed. The generation processing of a digital signature applies EC-DSA (Elliptic Curve Digital Signature Algorithm) under standard establishment for exampleby IEEE P1363. The title keydigital signatureand public key certification which were generated are stored in a recording medium (disk).
[0155]Nextby S307a title inherent key is generated from the above-mentioned disk inherent key and a title key (refer to drawing 16).
[0156]A recording and reproducing device receives S308 the encrypted data of the contents data which should be recorded in the form of a TS packet. By S309TS processing means 300 adds ATS which is the time information which received each TS packet. Or the value which combined the copy control information CCI and ATS and the information of further others is added. Nextit is judged whether the TS packet which added ATS was received one by one by S3101 block is formedfor examplethe identification data in which whether it having amounted to X= 32 and the end of a packet are shown was received. When one of conditions is satisfiedit progresses to Step S311and the packet to X individual or the end of a packet is put in orderand 1-block block data is formed.
[0157]Nextthe cipher-processing means 150 is S312 and generates the block key which is a key which enciphers the data of the block from 32 bits (block seed containing ATS) of the head of block dataand the title inherent key generated by S307 (refer to drawing 17).
[0158]In S313the block data formed by S311 using the block key is enciphered. As explained also in advanceit is the m+1st byte to final data of block data that it is the target of encryption. DES (Data Encryption Standard) as which an encryption algorithm is specifiedfor example by FIPS 46-2 is applied.
[0159]By S314the enciphered block data is recorded on a recording medium. By S315it is judged whether all the data was recorded. If all the data is recordedrecording processing is ended and all the data is not recordedit will return to S308 and processing of the remaining data will be performed.
[0160]Contents will be enciphered by the above processingit will be recorded on a recording mediumand the digital signature to the title key corresponding to enciphered content and a public key certification will be further recorded on a recording medium.
[0161]Although the digital signature was given to the title key in the above-mentioned examplea digital signature may be given to a title key and disk ID. By doing in this wayit can clarify that the data was recorded on the diskand that by which the data was copied to other disks can make easily judgment that it is an unjust copy.
[0162][Contents playback processing using a medium key] Nextdecoding of enciphered content data and regeneration which were stored in the recording medium are explained below using drawing 22.

[0163]In regenerationplayback equipment reads the public key certification and digital signature of a recorder which are first recorded with the contents data to reproduceand checks such justification.
[0164]That isif the justification of a public key certification is inspected using the public key (signature verification keys) of a reliable center which playback equipment holds and it succeeds in thisthe digital signature which the recorder created and recorded using the public key (signature verification keys) of a recorder contained in the public key certification will be inspected. As an inspection method of a digital signatureabove-mentioned EC-DSA can be usedfor example.
[0165]Nextplayback equipment reads the identification information (ID) of a recorder from the public key certification currently recordedand checks that RIBOKU (exclusion) of this recorder is not carried out from a system from this and RIBOKESHON information.
[0166](RIBOKU inspection using a RIBOKESHON list) As RIBOKESHON informationthe RIBOKESHON list shownfor example in drawing 23 can be used. A center gives a digital signature to the data which wrote together ID of the apparatus which carries out RIBOKU (exclusion) as a RIBOKESHON list is shown in a figureand the version number of a list. For examplethe memory of the apparatus (recording and reproducing device) by which 1 manufacture is carried out is made to memorize this RIBOKESHON list. It is made to circulate via a network or a recording medium together with 2 contents data. It enables it to acquire the RIBOKESHON information that playback equipment is newerby circulating the inside of a system by which method at the time of regeneration.
[0167]When using a RIBOKESHON listin order to inspect that a list is not what was forged and alteredverification processing of a signature of the center stored in the RIBOKESHON list is performed. The verification processing of a signature can be inspected like signature verification of a public key certification using the public key (signature verification keys) of the center which apparatus (recording and reproducing device) has beforehand.
[0168](RIBOKU inspection using EKB) It is good also as composition which does not take the composition distributed to each apparatus as a list as RIBOKESHON information shown in drawing 23 againbut distinguishes RIBOKU using EKB. For examplein the system by which apparatus has been arranged at the tree form shown in drawing 11it is assumed that EKB shown in the example 1 of (A) of drawing 12 was stored in the recording medium. If each apparatus sees the index of EKB one by one at this timehe can understand that what expressed with tree form the node key updated by EKB becomes like the thick line of drawing 24.
[0169]And he gets blocked only the apparatus located under the leaf (leaf) of the tree shown by the thick lineand that the updated node key can be obtained can understand that they are only the devices 01and 2. And RIBOKU [ the other apparatus / system ] can be judgedIt becomes possible to suspend redistribution of the record contents by RIBOKU apparatus by performing processing which forbids reproduction of the contents data which apparatus with these ID recorded

at the time of execution of regeneration. It is premised on the position of the leaf in drawing 11 and ID of a device corresponding in this example. That isthe existence of RIBOKU is distinguished by performing trace processing of the index of validation key blocks (EKB) based on said ID.
[0170]The RIBOKU inspection by trace processing is explained in detail. Firstthe example of a format of validation key blocks (EKB) is shown in drawing 25. The version 1001 is an identifier which shows the version of validation key blocks (EKB). A version has a function which shows the correspondence relation of the function and contents which identify the newest EKB. The depth 1002 shows the hierarchy number of the hierarchy tree to the device of the distribution destination of validation key blocks (EKB). The data pointer 1003 is a pointer in which the position of the data division in validation key blocks (EKB) is shown.
It is a pointer which the tag pointer 1004 shows the position of a tag part toand the signature pointer 1005 shows the position of a signature.

[0171]The data division 1006 stores the data which enciphered the node key updatedfor example. For exampleeach cryptographic key about the updated node key as shown in drawing 13 is stored.
[0172]The tag part 1007 is a tag in which the physical relationship of the node key and leaf key which were stored in the data divisionand which were enciphered is shown. The grant rule of this tag is explained using drawing 26. Drawing 26 shows the example which sends the validation key blocks (EKB) previously explained by drawing 12 (A) as data. The data at this time comes to be shown in the table (b) of drawing 26. Let the address of the top node contained in the cryptographic key at this time be a top node address. In this casesince updating key K(t) R of the route key is containeda top node address serves as KR. At this timethe data Enc (K(t) 0 and K (t) R) of the highest rung is in the position shown in the hierarchy tree shown in (a) of drawing 26for example. Herethe following data is Enc (K (t) 00K(t)0). It is in the position at the lower left of front data on a tree.
A tag is set upand 1 is set up when there is dataand there is nothing0 and. A tag is set up as [a left (L) tag and a right (R) tag]. Since there is data in the left of the data Enc (K(t) 0 and K (t) R) of the highest rung and there is no data in L tag =0 and the rightit is set to R tag =1. Hereaftera tag is set as all the data and the data row shown in drawing 26 (c) and a tag sequence are constituted.
[0173]A tag is a key arrangement identification tag set up in order to show where [ of a tree structure ] the data Enc (KxxxKyyy) is located. the key data Enc (KxxxKyyy) stored in a data division -- since ... is only enumeration data of the key enciphered simplyit enables distinction of the position on the tree of the cryptographic key stored as data with the tag mentioned above. The node index to which encryption data was made to correspond like composition of that previous drawing 12 explained is usedwithout using the tag mentioned abovefor exampleit is
0:Enc (K(t) 0 and K (t) root).
00:Enc(K(t)00K(t)0
000:Enc(K((t)000K(T)00)

Although it is also possible to consider it as a data configuration like ...in the distribution etc. which it will become redundant data and data volume will increase if it has composition using such an indexand pass a networkit is not desirable. On the other handdistinction of a key position is attained with small data volume by using the tag mentioned above as index data in which a key position is shown.
[0174]It returns to drawing 25 and an EKB format is explained further. A signature (Signature) is an electronic signature which the EKB issue office which published validation key blocks (EKB)for examplea certificate authoritya lock management centercontents ROBAIDAa settlement-of-accounts organizationetc. perform. It checks that the devices which received EKB are the validation key blocks (EKB) which the just validation key-blocks (EKB) publisher published by signature verification.
[0175]The tag stored in EKB so that I might be understood from the explanation about drawing 26 shows 0 or 1 existence of the key data of the left of a self-nodeand a right node. That iswhen there is datathe case where there are not 0 and data is set up as 1. The tracking processing of EKB based on leaf IDi.e.how to followis performed using the tag based on such conditioning.
[0176]Pursuit (how to follow) of EKB based on leaf ID is explained using drawing 27. Let the device which has the leaf key K1001 as shown in drawing 27 (a) be a RIBOKU device [1001]. At this timeEKB has the composition of a cryptographic key like drawing 27 (b)and a tag. EKB of drawing 27 (b) turns into EKB which updated KRK1K10and K100in order RIBOKU [ one device [1001] of drawing 27 (a) ].
[0177]By processing this EKBall leaves other than a RIBOKU device [1001] can acquire updated route key K(t) R. That issince the leaf which stands in a row in the low rank of the node key K0 holds in a device the node key K0 which is not updatedthe acquisition of updating route key K(t) R of it is attained by decoding Enc (K0K(t) R) by K0. The leaf not more than K11 acquires updating node key K(t)1 using K11 which is not updated by decoding Enc (K11K(t)1) by K11An updating route key is acquirable by decoding Enc (K(t) 1 and K (t) R) by K(t)1. Only by one decoding step increasing also about the low rank leaf of K101an updating route key is acquirable similarly.
[0178]It is a self leaf keyand the device [1000] with the leaf key [ RIBOKU / leaf key ] K1000 decodes Enc (K1000K(t)100)after acquiring K(t)100it decodes the node key of a higher rank one by oneand can acquire an updating route key.
[0179]RIBOKU -- having had -- a device -- [-- 1001 --] -- self -- a leaf -- one -- a step -- a top -- updating -- a node key -- K -- (-- t --) -- 100 -- EKB -- processing -- being unacquirable -- since -- after all -- updating -- a route -- a key -- K -- (-- t --) -- R -- being unacquirable .
[0180]The data division shown in drawing 27 (b) and EKB which has a tag are distributed to the just device [ RIBOKU / device ] from an EKB issue officeand it is stored in the device.
[0181]The device which tries to perform RIBOKU verification acquires ID from a public key certification after verification of the public key certification of the

RIBOKU device [ID=1001] of drawing 27 (a). This ID is [1001] and shows the leaf position of EKB distribution tree composition.
[0182]The device which took out ID [1001] verifies whether the device corresponding to the leaf of ID=1001 is set up as an effective leaf device in EKB. It performs as processing which judges whether route key K(t) R by which this verification [1001]i.e.a leafwas updated is acquirable.
[0183]For exampleif it is a leaf belonging to the low rank of the renewal node keys of un-(K0 of ex. drawing 27 (a)K11etc.)When it is a leaf which can judge if RIBOKU is clear and it is a just deviceand belongs to the low rank of an updating node keyA judgment RIBOKU [ whether the encryption data which can acquire the updating node key is stored in EKB / the entity ] is attained.
[0184]The example which performs EKB tracking processing as an example of decision processing based on the tag stored in EKB is explained. EKB tracking processing is processing which judges whether a key distribution tree can be followed from the route key of a higher rank. For exampleaccording to a lower bita tree is followed for [1001] which is ID of the leaf [1001] of drawing 27 as 4 bits of [1][0][0]and [1] one by one from the most significant bit. If a bit is 1 and it is right-hand side and 0it will progress to the left.
[0185]From the route of drawing 27 (a)the most significant bit of ID [1001] is 1and goes to right-hand side. The tag of the beginning in EKB is 0: {00}and having data on both branches is judgedit goes to right-hand sideand it is followed and stuck to K1. Nextit progresses to the node of the low rank of K1. The 2nd bit of ID [1001] is 0 and goes to left-hand side. It is 2: {00} of drawing 27 (a) and (b)and it judges that the tag in which the data existence of the low rank of K1 is shown has data on both branchesand it goes to left-hand sideand is followed and stuck to K10. The 3rd bit of ID [1001] is 0 and goes to left-hand side. It is 3: {00} of drawing 27 (a) and (b)and it judges that the tag in which the data existence of the low rank of K10 is shown has data on both branchesand it goes to left-hand sideand is followed and stuck to K100. The least significant bit of ID [1001] is 1and goes to right-hand side. The tag in which the data existence of the low rank of K100 is shown is 5: {01} of drawing 27 (a) and (b)and does not have data in right-hand side. thereforearrive at a node [1001] -- it is judged that there is nothing and it is judged with the device of ID [1001] being the device which cannot acquire the updating route key by EKBi.e.a RIBOKU device.
[0186]For exampleif the device ID which has the leaf key K1000 of drawing 27 (a) is [1000] and the EKB tracking processing based on the tag in the same EKB as ****i.e.the processing which follows a treeis performedSince it can arrive at a node [1000]it is judged with it being a just device [ RIBOKU / device ] which can acquire the updating route key by EKB.
[0187]arrive also at the leaf of low rankssuch as the node key which is not updatedfor examplefor exampleK0and K11at the leaf itself -- although there is nothingit is possible to arrive at the end node which is not updated in this case. Since processing of EKB is possible for the leaf of the low rank of the node which is not updated and it can acquire an updating route key using the node key which

is not updatedit is a just device. It becomes possible [ judging with the tag corresponding to the node ] whether it is a node key which is not updated. The tag corresponding to the node key K0 which is not updatedK11and K101 is set to 1: {11}4: {11}and 6 {11}and although a low order node or a leaf exists furthertheseNot having enciphered key data in EKB is shownand it is judged with the device of the leaf of the low rank of these being an effective just device [ RIBOKU / device ].
[0188]Although the example shown in drawing 27 is a RIBOKU mode only about one deviceit is also possible RIBOKU [ all the leaf devices which are under a certain node as shown in drawing 28 ] collectively. The data (cryptographic key) of EKB in this case and a tag become like drawing 28 (b).
[0189]For examplesupposing it acquires ID [1000] from the public key certification of the leaf device corresponding to K1000 [ RIBOKU / 1000 / the device ]processing which follows a tree based on the tag of EKB based on this ID [1000] will be performed.
[0190]From the route of drawing 28 (a)the most significant bit of ID [1000] is 1and goes tc right-hand side. It is tag 0of the beginning in EKB: {00}and having data on both branches is judgedit goes to right-hand sideand it follows and sticks to K1. Nextit progresses to the node of the low rank of K1. The 2nd bit of ID [1000] is 0 and goes to left-hand side. The tag in which the data existence of the low rank of K1 is shown is 2: {10} of drawing 13 (a) and (b)and does not have data in left-hand side. thereforearrive at a node [1000] -- there is nothing. The tags corresponding to the end node K1 at this time are {10}and are not {11} without low-ranking data.
[0191]The tag {10} shows that the enciphered key data for acquiring K1 (t) which can be decoded and which was updated only in the right-hand side low-ranking node or leaf of K1 is stored in EKB.
[0192]Thusthe final point which arrives based on leaf ID is a nodeand when the correspondence tag of the last node has values other than {11}having low-ranking enciphered key data in EKB further is shown. In this casesince the leaf device with that ID cannot acquire the route key updated by processing of EKBit is judged with it being the device [ RIBOKU / device ].
[0193]Thusit becomes possible to judge RIBOKU [ the communications partner ] based on leaf ID stored in the public key certification acquired from the communications partner in authenticating processing.
[0194]The process flow using EKB about RIBOKU device decision processing is shown in drawing 29. Each step of a flow is explained. In Step S351ID is acquired from a public key certification to be examined. In Step S352tracking processing aiming at the leaf or lead which ID shows based on the tag of EKB using acquired ID is performed.
[0195]Tracking processing is performed in the procedure explained using above-mentioned drawing 27 and drawing 28. as a result of tracking processingarrive at the leaf or node which ID showsor arrive -- even if it is a case where there is nothingin the leaf or node which ID showsit is judged whether acquisition of whether EKB processing is possible and an updating route key is possible (S353).
[0196]If judged with it being ID in the position in which EKB processing is

possibleit will progress to Step S354 and will judge with the device corresponding to ID being a just device [ RIBOKU / device ]. If judged with it being ID which is in the position in which EKB processing is impossible on the other handit will progress to Step S355 and will judge with the device corresponding to ID being an inaccurate device [ RIBOKU / device ].

[0197]In above-mentioned tracking processingalthough the tag part of EKB usesthe data division does not use. Size of EKB for them can be made small by using not the usual EKB shown in drawing 25 but EKB without a data division using thisin order to express RIBOKESHON information. Of courseit is also possible to use EKB for protecting the usual contents shown in drawing 25since RIBOKESHON information is expressed.

[0198]As mentioned abovethat verification which does not require RIBOKU [ the apparatus which recorded contents to the recording medium by the RIBOKU inspection according to a RIBOKESHON list or trace processing of an EKB tree ] is performed. On condition that RIBOKU [ the apparatus which recorded contents ] was verifiedplayback equipment continues regeneration of contents data. Like the encryption and recording processing which were explained using drawing 14from a medium key and disk IDin regenerationgenerate a disk inherent key and A disk inherent keyA title inherent key is generated from a title keyfurtherfrom a title key and the block seed read in a recording mediuma block key is generated and decoding processing of the encryption data of the block unit read in the recording medium 200 is performedusing a block key as a decryption key.

[0199]The outline of regeneration is explained using the flow chart of drawing 30. Firstin Step S401playback equipment performs the public key certification of a storing salmon **** contents recording deviceand verification of a digital signature to the recording medium which recorded reproduction object contents. After performing the center signature of a public key certification using the public key of a center and checking the justification of a public key certification firstverification takes out the public key of the contents recording device stored in the public key certificationand performs verification of a contents recording person's digital signature. Any verification follows that to the following step by O.K.if one of verification is NGsubsequent stepwise execution is forbidden and regeneration is stopped.

[0200]Nextthe RIBOKESHON inspection of a contents recording device is performed in Step S402. This RIBOKESHON inspection is conducted by inspecting whether apparatus ID stored in the RIBOKESHON list shown in drawing 23 beforehand stored in playback equipmentfor example and apparatus ID in a public key certification have a match. Or tree search processing by the above-mentioned EKB tree composition may be performed. If judged with RIBOKU [ the contents recording device ] in the RIBOKESHON inspection of Step S402when RIBOKU [ the following step / progress and ]subsequent stepwise execution is forbidden and regeneration is stopped.

[0201]When judged with RIBOKU [ the contents recording device ] in the

RIBOKESHON inspection of Step S402In Step S403read-out from the recording medium of enciphered content is performeddecoding processing of enciphered content is performed in Step S404and reproduction of contents is performed.
[0202]Thussince it had composition which performs only reproduction of the contents recorded by the apparatus [ RIBOKU / apparatus / by judging the RIBOKU situation of a contents recording device ] on the occasion of the contents playback processing stored in the recording mediumIt is prevented that circulation use of the contents recorded unjustly is carried out disorderly. A RIBOKU judging is judged by ID stored in the public key certificationand the reliability is maintained.
[0203]Nextthe detailed processing in the case of performing reproduction of the record contents by which the digital signature was performed to enciphered content using drawing 31 is explained.
[0204]In Step S501playback equipment reads a medium key and disk ID from a recording mediumand performs read-out of a title keya digital signatureand a public key certification in Step S502. When a signature and a public key certification do not exist (S503:No)it is judged with their not being the contents by just recording processingexecution of subsequent processings is suspendedand regeneration is ended.
[0205]When a signature and a public key certification exist (S503:Yes)verification of a public key certification is performed in Step S504. Verification of a public key certification is performed using the public key of the center (certificate authority) which performs issue management of the public key certification which playback equipment holds. Verification of a public key certification is O.K.and if justification is checkedit will progress to the following step. When justification verification is NGexecution of subsequent processings is suspended and regeneration is ended.
[0206]Nextin Step S505the identifier (ID) of a recorder which performed contents recording is taken out from a public key certificationand a RIBOKU inspection is conducted. A RIBOKU inspection is performed by either Libor Christo of above-mentioned drawing 23or tree search processing. If judged with there being no RIBOKU of the recorder of contentsit will progress to the following stepand if judged with those with RIBOKUexecution of subsequent processings will be suspended and regeneration will be ended.
[0207]Nextin S506a disk inherent key is generated using a medium key and disk ID. It asks to have explained the disk inherent key previously by applying the method of using hash function SHA-1 defined by FIPS 180-1the method (refer to drawing 15) of using the hash function based on a block cipheretc.
[0208]Nextit progresses to S507 and a title inherent key is generated from the title key which read and read the title key (Title Key)and a disk inherent key (refer to drawing 16).
[0209]In S508playback equipment reads the block data of the contents data which should be reproduced. It reads by S509 and judges whether a block is the 1st blockand in being the 1st blockit performs verification of a contents recording person's (recorder) digital signature generated to the 1st block in Step S510.

Verification of a digital signature is performed using the public key of the contents recording device picked out from the public key certification in which justification was verified. Verification of a digital signature is O.K.and if justification is checkedit will progress to the following step. When justification verification is NGexecution of subsequent processings is suspended and regeneration is ended.
[0210]In Step S511the block key which is a key which decodes the data of the block is generated from 32 bits (block seed containing ATS) of the head of block dataand the title inherent key generated by S507 (refer to drawing 17).
[0211]In S512block data is decoded using a block key. DES (Data Encryption Standard) as which a decoding algorithm is specifiedfor example by FIPS 46-2 is applied.
[0212]By S513it is judged whether all the data was read. If all the data is readregeneration is ended and all the data is not readit will return to S508 and processing of the remaining data will be performed.
[0213]Thusverification of a public key certificationthe judgment of RIBOKU of a contents recording deviceSequential execution of the verification of the digital signature to the block data of enciphered content will be carried outthe justification of contents will be judged based on all the conditions having been satisfiedand decoding from the recording medium of enciphered content and regeneration will be performed.
[0214]Nextthe detailed processing in the case of performing reproduction of the record contents by which the digital signature was performed to the title key using drawing 32 is explained.
[0215]In Step S601playback equipment reads a medium key and disk ID from a recording mediumand performs read-out of a title keya digital signatureand a public key certification in Step S602. When a signature and a public key certification do not exist (S603:No)it is judged with their not being the contents by just recording processingexecution of subsequent processings is suspendedand regeneration is ended.
[0216]When a signature and a public key certification exist (S603:Yes)verification of a public key certification is performed in Step S604. Verification of a public key certification is performed using the public key of the center (certificate authority) which performs issue management of the public key certification which playback equipment holds. Verification of a public key certification is O.K.and if justification is checkedit will progress to the following step. When justification verification is NGexecution of subsequent processings is suspended and regeneration is ended.
[0217]Nextin Step S605the identifier (ID) of a recorder which performed contents recording is taken out from a public key certificationand a RIBOKU inspection is conducted. A RIBOKU inspection is performed by either Libor Christo of above-mentioned drawing 23or tree search processing. If judged with there being no RIBOKU of the recorder of contentsit will progress to the following stepand if judged with those with RIBOKUexecution of subsequent processings will be suspended and regeneration will be ended.
[0218]Nextverification of a contents recording person's (recorder) digital signature

performed to the title key in Step S606 is performed. Verification of a digital signature is performed using the public key of the contents recording device picked out from the public key certification in which justification was verified. Verification of a digital signature is O.K.and if justification is checkedit will progress to the following step. When justification verification is NGexecution of subsequent processings is suspended and regeneration is ended.

[0219]Nextin S607a disk inherent key is generated using a medium key and disk ID. It asks to have explained the disk inherent key previously by applying the method of using hash function SHA-1 defined by FIPS 180-1the method (refer to drawing 15) of using the hash function based on a block cipheretc.

[0220]Nextit progresses to S608 and a title inherent key is generated from the title key which read and read the title key (Title Key)and a disk inherent key (refer to drawing 16).

[0221]In S609playback equipment reads the block data of the contents data which should be reproduced. In Step S610the block key which is a key which decodes the data of the block is generated from 32 bits (block seed containing ATS) of the head of block dataand the title inherent key generated by S608 (refer to drawing 17).

[0222]In S611block data is decoded using a block key. DES (Data Encryption Standard) as which a decoding algorithm is specifiedfor example by FIPS 46-2 is applied.

[0223]By S612it is judged whether all the data was read. If all the data is readregeneration is ended and all the data is not readit will return to S609 and processing of the remaining data will be performed.

[0224]Thusverification of a public key certificationthe judgment of RIBOKU of a contents recording deviceSequential execution of the verification of the digital signature to the title key of enciphered content will be carried outthe justification of contents will be judged based on all the conditions having been satisfiedand decoding from the recording medium of enciphered content and regeneration will be performed.

[0225]As mentioned abovein the encryption processing at the time of the record over the recording medium of contents dataand the decoding processing at the time of the reproduction from a recording mediumBased on the medium key which computed the medium key based on EKB and was computed after thatother identifiersetc.the key for encryption processing of contents or the key for decoding processings is generated.

[0226]Although the example mentioned above explained the composition which generates the key used for contents data encryption processing and decoding processing using a medium keyIt is good also as composition which generates the key which acquires not a medium key but a master key common to two or more recording and reproducing devicesor debye skiing peculiar to a record reproducer from EKBand uses it for contents data encryption processing and decoding processing based on these. It is also possible to apply as the medium key acquired from EKBa master keyor a key which uses the debye skiing itself for encryption

processing of contents data and decoding processing.
[0227]As mentioned abovein this inventionwhen a recording and reproducing device recorded data on an information recording mediuman own digital signature and public key certification were recorded with data. Since he is trying to also certainly record with data proof which recorder recordedby this when recording informationSince it can specify which recorder recorded it even if the recording medium containing the data recorded unjustly circulatedexclusion from a system can be performed.
[0228]When a recording and reproducing device reads dataafter checking the justification of the above-mentioned digital signature and the public key certification and checking RIBOKU [ the recorder / system ] furtherit had composition which reads data. While the inaccurate recorder is delivering the powerless thing an attack which does not record a digital signature to inaccurate record data by thisexclusion from the system of an inaccurate device is more powerfully performed by making it not reproduce the data recorded with an inaccurate device with a just device.
[0229][Copy control in recording processing Nowin order to protect profitssuch as an owner of a copyright of contentsin the licensed deviceit is necessary to control the copy of contents.]
[0230]That isto record contents on a recording mediumthe contents investigate whether it is what may be copied (a copy is possible)and it is necessary to make it record only the contents which may be copied. When reproducing and outputting the contents recorded on the recording mediumthe illegal copy of the contents to output needs to be made not to be carried out later.
[0231]Thenprocessing of the recording and reproducing device of drawing 1 in the case of performing record reproduction of contents is explained with reference to the flow chart of drawing 33 and drawing 34performing copy control of such contents.
[0232]Firstwhen recording the contents of the digital signal from the outside on a recording mediumrecording processing according to the flow chart of drawing 33 (A) is performed. Processing of drawing 33 (A) is explained. The record reproducer 100 of drawing 1 is explained as an example. If the contents (digital contents) of a digital signal are supplied to input-and-output I/F120 via an IEEE1394 serial bus etc.in Step S701input-and-output I/F120 will receive the digital contentsand they will follow it to Step S702for example.
[0233]In Step S702it is judged whether the digital contents which received can copy input-and-output I/F120. That isthe contents are judged [ that it can copy and ] when the contents which input-and-output I/F120 received are not enciphered for example (for examplewhen the contents of a plaintext are supplied to input-and-output I/F120without using above-mentioned DTCP).
[0234]It shall suppose that the recording and reproducing device 100 is a device based on DTCPand processing shall be performed according to DTCP. 2-bit EMI (Encryption Mode Indicator) as copy control information for controlling a copy is prescribed by DTCP. When EMI is 00B (B expresses that the value before that is a

binary number)Contents express that it is copy-free (Copy-freely)and when EMI is 01Bcontents express that it is what (No-more-copies) cannot carry out the copy beyond it. It expresses that contents are what (Copy-one-generation) may be copied only once when EMI is 10Band when EMI is 11Bcontents express that it is what (Copy-never) the copy is forbidden.

[0235]EMI is contained in the signal supplied to input-and-output I/F120 of the recording and reproducing device 100and contents are judged [ that it can copy and ] when the EMI is Copy-freely and Copy-one-generation. Contents are judged [ that it cannot copy and ] when EMI is No-more-copies and Copy-never.

[0236]In Step S702when judged [ that contents cannot be copied and ]Steps S703-S705 are skippedand recording processing is ended. Thereforecontents are not recorded on the recording medium 10 in this case.

[0237]In Step S702when judged [ that contents can be copied and ]it progresses to Step S703 and processing in Step S12 of drawing 3 (A)S13and S14 and same processing are hereafter performed in Steps S703-S705. That isATS addition to the transport packet by TS processing means 300 and encryption processing in the cipher-processing means I50 are performedthe enciphered content obtained as a result is recorded on the recording medium 195and recording processing is ended.

[0238]EMI is contained in the digital signal supplied to input-and-output I/F120. When digital contents are recordedthe informationincluding for exampleembedded CCI in DTCPetc.which expresses a copy control state like EMI or EMI with the digital contents is also recorded.

[0239]Under the present circumstancesgenerallythe information showing Copy-One-Generation is changed and recorded on No-more-copies so that the copy beyond it may not be allowed.

[0240]In the recording and reproducing device of this inventioncopy control informationsuch as this EMIembedded CCIetc.is recorded in the form added to a TS packet. That islike Example 2 of drawing 10or Example 332 bits which added 24 bits thru/or 30 bitsand copy control information for ATS are added to each TS packetas shown in drawing 5.

[0241]When recording the contents of the analog signal from the outside on a recording mediumrecording processing according to the flow chart of drawing 33 (B) is performed. Processing of drawing 33 (B) is explained. When the contents (analog content) of an analog signal are supplied to input-and-output I/F140input-and-output I/F140In Step S711the analog content which received the analog contentand progressed and received to Step S712 judges whether it can copy or not.

[0242]Here the decision processing of Step S712 to the signal received by input-and-output I/F140for example. It is carried out based on whether a macro vision (Macrovision) signal and a CGMS-A (Copy Generation Management System-Analog) signal are included. That iswhen a macro vision signal is recorded on the video cassette tape of a VHS methodit is a signal which serves as a noise.

Analog content is judged [ that it cannot copy and ] when this is contained in the signal received by input-and-output I/F140.

[0243]For examplea CGMS-A signal is a signal which applied the CGMS signal used for the copy control of a digital signal to the copy control of the analog signalIt is expressed any of what (Copy-freely) has a free copy of contentsthe thing (Copy-one-generation) which may be copied only onceor the things (Copy-never) to which the copy is forbidden they are.
[0244]Thereforeanalog content is judged [ that it can copy and ]when a CGMS-A signal is included in the signal received by input-and-output I/F140 and the CGMS-A signal expresses Copy-freely and Copy-one-generation. Analog content is judged [ that it cannot copy and ] when the CGMS-A signal expresses Copy-never.
[0245]Analog content is judged [ that it can copy and ] when a macro vision signal and CGMS-A signal is not included in the signal received by input-and-output I/F4 for exampleeither.
[0246]In Step S712when judged [ that analog content cannot be copied and ]Steps S713 thru/or S717 are skippedand recording processing is ended. Thereforecontents are not recorded on the recording medium 10 in this case.
[0247]In [ when judged / that analog content can be copied and / progress to Step S713 in Step S712and ] the following and Steps S713 thru/or S717Processing in Steps S22 thru/or S26 of drawing 3 (B) and same processing are performedand therebydigital conversionMPEG codingTS processingand encryption processing are madeand contents are recorded on a recording mediumand end recording processing.
[0248]When the CGMS-A signal is included in the analog signal received by input-and-output I/F140 and analog content is recorded on a recording mediumthe CGMS-A signal is also recorded on a recording medium. That isthis signal is recorded on the portion of the information on CCI shown by drawing 10or others. Under the present circumstancesgenerallythe information showing Copy-One-Generation is changed and recorded on No-more-copies so that the copy beyond it may not be allowed. Howeverit is not this limitation when a rulesuch as "treating the copy control information of Copy-one-generation as No-more-copies although recorded without changing into No-more-copies"is decided in the system.
[0249][Copy control in regeneration] Nextwhen reproducing the contents recorded on the recording medium and outputting outside as digital contentsregeneration according to the flow chart of drawing 34 (A) is performed. Processing of drawing 34 (A) is explained. In Step S801S802and S803processing in Step S31 of drawing 4 (A)S32and S33 and same processing are performed firstand by thisIn the cipher-processing means 150decoding processing is made for the enciphered content read from the recording mediumand TS processing is made. The digital contents by which each processing was performed are supplied to input-and-output I/F120 via the bus 110.
[0250]Input-and-output I/F120 judges whether it is what the digital contents

supplied there can copy later in Step S804. That isthe contents are judged [ that it can copy later and ] when the information (copy control information) which expresses a copy control state to the digital contents supplied to input-and-output I/F120 like EMI or EMIfor example is not included.
[0251]When EMI is contained in the digital contents supplied to input-and-output I/F120 for exampleThereforewhen EMI is recorded according to the standard of DTCP at the time of record of contents. Digital contents are judged [ that it can copy later and ] when the EMI (recorded EMI (Recorded EMI)) is Copy-freely. Contents are judged [ that it cannot copy later and ] when EMI is No-more-copies.
[0252]Generally recorded EMI is neither Copy-one-generation nor Copy-never. It is because the digital contents which EMI of Copy-one-generation is changed into No-more-copies at the time of recordand have EMI of Copy-never are not recorded on a recording medium. Howeverit is not this limitation when a rulesuch as "treating the copy control information of Copy-one-generation as No-more-copies although recorded without changing into No-more-copies"is decided in the system.
[0253]In Step S804when contents are judged [ that it can copy later and ]it progresses to Step S805and input-and-output I/F120 outputs the digital contents outsideand ends regeneration.
[0254]When contents are judged [ that it cannot copy later and ] in Step S804progress to Step S806 and input-and-output I/F120For exampleaccording to the standard of DTCPetc.it outputs outside in the form where digital contents are not copied to the digital contents laterand regeneration is ended.
[0255]Namelywhen EMI recorded as mentioned abovefor example is No-more-copies (or although the copy control information of "Copy-one-generation is recorded in a systemwithout changing into No-more-copies) The rule of treating as No-more-copies" is decidedand when EMI recorded under the conditions is Copy-one-generationas for contentsthe copy beyond it is not allowed.
[0256]For this reasoninput-and-output I/F120 attests mutually between a partner's devices according to the standard of DTCPwhen a partner is a just deviceenciphers digital contents (when it is a device based on the standard of DTCP here)and outputs them outside.
[0257]Nextwhen reproducing the contents recorded on the recording medium and outputting outside as analog contentregeneration according to the flow chart of drawing 34 (B) is performed. Processing of drawing 34 (B) is explained. In Steps S811 thru/or S815processing in Steps S41 thru/or S45 of drawing 4 (B) and same processing are performed. That isread-out of enciphered contentdecoding processingTS processingMPEG decodingand D/A conversion are performed. The analog content obtained by this is received by input-and-output I/F140.
[0258]Input-and-output I/F140 judges whether it is what the contents supplied there can copy later in Step S816. That isthe contents are judged [ that it can copy later and ] when copy control informationsuch as EMIis not recorded on the contents currently recorded together for example.
[0259]Contents are judged [ that it can copy later and ]when EMI or copy control

information is recordedfor example according to the standard of DTCP at the time of record of contents and the information is Copy-freely.
[0260]When EMI or copy control information is No-more-copiesin a systemrecord the copy control information of "Copy-one-generationwithout changing into No-more-copiesbut. The rule of treating as No-more-copies" is decidedand contents are judged [ that it cannot copy later and ] when EMI or copy control information recorded under the conditions is Copy-one-generation.
[0261]When a CGMS-A signal is included in the analog content supplied to input-and-output I/F140 for exampleThereforeanalog content is judged [ that it can copy later and ]when a CGMS-A signal is recorded with the contents at the time of record of contents and the CGMS-A signal is Copy-freely. Analog content is judged [ that it cannot copy later and ] when a CGMS-A signal is Copy-never.
[0262]In Step S816when contents are judged [ that it can copy later and ]it progresses to Step S817and input-and-output I/F140 outputs outside the analog signal supplied there as it isand ends regeneration.
[0263]In Step S816when contents are judged [ that it cannot copy later and ]it progresses to Step S818and input-and-output I/F140 is outputted outside in the form where analog content is not copied to the analog content laterand ends regeneration.
[0264]Namelywhen copy control informationsuch as EMI recorded as mentioned abovefor exampleis No-more-copies (or) Although the copy control information of "Copy-one-generation is recorded in a systemwithout changing into No-more-copiesThe rule of treating as No-more-copies" is decidedand when copy control informationsuch as EMI recorded under the conditionsis Copy-one-generationas for contentsthe copy beyond it is not allowed.
[0265]For this reasoninput-and-output I/F140 adds the GCMS-A signal with which a macro vision signal and Copy-never are expressed for analog content at itfor exampleand outputs it outside. For examplealso when the recorded CGMS-A signal is Copy-neveras for contentsthe copy beyond it is not allowed. For this reasoninput-and-output I/F140 changes a CGMS-A signal into Copy-neverand outputs it outside with analog content.
[0266]As mentioned aboveit becomes possible by performing record reproduction of contents to prevent the copy (illegal copy) besides the range which contents were allowed from being performedperforming copy control of contents.
[0267][Composition of a data processing means] Software can also perform as well as in addition performing a series of processings mentioned above by hardware. That isit is also possible tohave composition performed by making a general-purpose computer and the microcomputer of one chip execute a program for examplealthough the cipher-processing means 150 can also be constituted as encryption/decoding LSI. TS processing means 300 can perform processing with software similarly. When software performs a series of processingsthe program which constitutes the software is installed in a general-purpose computerthe microcomputer of one chipetc. Drawing 35 shows the example of composition of the 1 embodiment of the computer by which the program which performs a series

of processings mentioned above is installed.
[0268]A program is recordable on hard disk [ as a recording medium ] 2005and ROM2003 built in the computer beforehand. A program Or a floppy (registered trademark) diskCD-ROM (Compact Disc Read Only Memory)It is temporarily or permanently storable in the removable recording media 2010such as MO (Magneto optical) diskDVD (Digital Versatile Disc)a magnetic diskand semiconductor memory (record). Such a removable recording medium 2010 can be provided as what is called a software package.
[0269]Install a program in a computer from the removable recording medium 2010 which was mentioned aboveand also via the artificial satellite for the digital satellite broadcasting from a download siteVia networks [ **** / transmitting to a computer on radio ]such as LAN (Local AreaNetwork) and the InternetIt transmits to a computer with a cableand in a computerit can receive in the communications department 2008 and the program transmitted by making it such can be installed on the hard disk 2005 to build in.
[0270]The computer contains CPU(Central Processing Unit) 2002. The input/output interface 2011 is connected to CPU2002 via the bus 2001. CPU2002 via the input/output interface 2010 by a user. If instructions are inputted by operating the input part 2007 which comprises a keyboarda mouseetc.according to itthe program stored in ROM(Read Only Memory) 2003 will be executed.

[0271]Or a program by which CPU2002 is stored in the hard disk 2005A program which was transmitted from the satellite or the networkwas received in the communications department 2008and was installed on the hard disk 2005Or the program which was read from the removable recording medium 2010 with which the drive 2009 was equippedand was installed on the hard disk 2005 is loaded to RAM(Random Access Memory) 2004and is executed.
[0272]TherebyCPU2002 performs processing performed by the composition of the block diagram according to the flow chart mentioned above processed or mentioned above. CPU2002 the processing result and via the input/output interface 2011 if neededIt is made to record on an output or the transmission from the communications department 2008and also the hard disk 2005 from the outputting part 2006 which comprises LCD (Liquid CryStal Display)a loudspeakeretc.
[0273]The processing step which describes the program for making various kinds of processings perform to a computer in this Description hereIt is not necessary to necessarily process to a time series in accordance with the order indicated as a flow chartand a parallel target or the processing (for exampleparallel processing or processing by an object) performed individually is also included.
[0274]A program may be processed by the computer of 1 and distributed processing may be carried out by two or more computers. A program may be transmitted to a distant computer and may be executed.
[0275]Although this embodiment explained as a center the example which

constitutes the block which performs encryption/decoding of contents from encryption/decoding LSI of one chipThe block which performs encryption/decoding of contents can also be realized as one software module which CPU170 shown in drawing 1 performsfor example. It is possible similarly to also realize processing of TS processing means 300 as one software module which CPU170 performs.

[0276]As mentioned aboveit has explained in detail about this inventionreferring to specific working example. Howeverit is obvious that a person skilled in the art can accomplish correction and substitution of this working example in the range which does not deviate from the gist of this invention. That iswith the gestalt of illustrationthis invention has been indicated and it should not be interpreted restrictively. In order to judge the gist of this inventionthe column of the Claims indicated at the beginning should be taken into consideration.

[0277]

[Effect of the Invention]As mentioned aboveas explainedwhen the Information Storage Division device records data on an information recording medium according to the composition of this inventionan own digital signature and public key certification are recorded with data. By thiswhen recording informationproof which recorder recorded was also always recorded with data. It checks that an information reproducing device checks the justification of a signature and a public key certificationand specifies a contents recording person before the decoding processing of contentsand there is no alteration of a public key certification and a digital signature in it. By this compositionefficient exclusion of use (reproduction) of the record contents by an inaccurate recorder is attained. Since it can specify which recorder recorded it even if the recording medium containing the data recorded unjustly circulatedexclusion from a system can be performed.

---

## DESCRIPTION OF DRAWINGS

---

[Brief Description of the Drawings]

[Drawing 1]It is a block diagram showing the example of composition of the Information Storage Division playback equipment of this invention.

[Drawing 2]It is a figure showing the example of the public key certification applied in the Information Storage Division playback equipment of this invention.

[Drawing 3]It is a figure showing the Data Recording Sub-Division process flow of the Information Storage Division playback equipment of this invention.

[Drawing 4]It is a figure showing the data reproduction process flow of the Information Storage Division playback equipment of this invention.

[Drawing 5]It is a figure explaining the data format processed in the Information Storage Division playback equipment of this invention.

[Drawing 6]It is a block diagram showing the composition of the transport stream (TS) processing means in the Information Storage Division playback equipment of this invention.

[Drawing 7]It is a figure explaining the composition of the transport stream processed in the Information Storage Division playback equipment of this invention.
[Drawing 8]It is a block diagram showing the composition of the transport stream (TS) processing means in the Information Storage Division playback equipment of this invention.
[Drawing 9]It is a block diagram showing the composition of the transport stream (TS) processing means in the Information Storage Division playback equipment of this invention.
[Drawing 10]It is a figure showing the example of composition of the block data as additional information of block data processed in the Information Storage Division playback equipment of this invention.
[Drawing 11]It is a tree lineblock diagram explaining the EKB message distribution processing to the Information Storage Division playback equipment of this invention.
[Drawing 12]It is a figure showing the example of EKB used for the key distribution to the Information Storage Division playback equipment of this invention.
[Drawing 13]It is a figure showing the example of distribution which uses EKB of the medium key in the Information Storage Division playback equipment of this inventionand the example of decoding processing.
[Drawing 14]It is a block diagram explaining the encryption processing at the time of the Data Recording Sub-Division processing which uses the medium key in the Information Storage Division playback equipment of this invention.
[Drawing 15]It is a figure which illustrates the example of generation of an applicable disk inherent key in the Information Storage Division playback equipment of this invention.
[Drawing 16]In the Information Storage Division playback equipment of this inventionit is a figure showing the example of generation processing of an applicable title inherent key.
[Drawing 17]It is a figure which illustrates the generation method of an applicable block key in the Information Storage Division playback equipment of this invention.
[Drawing 18]It is a block diagram explaining the encryption processing at the time of the Data Recording Sub-Division processing in the Information Storage Division playback equipment of this invention.
[Drawing 19]It is a flow chart explaining the processing which generates the signature to enciphered content in the Information Storage Division playback equipment of this inventionand performs Data Recording Sub-Division.
[Drawing 20]It is a figure showing the example of composition of the enciphered content recorded in the Information Storage Division playback equipment of this inventionand the table which manages correspondence with a public key certificationa signatureetc.
[Drawing 21]It is a flow chart explaining the processing which generates the signature to a title key in the Information Storage Division playback equipment of this inventionand performs Data Recording Sub-Division.
[Drawing 22]It is a block diagram explaining the decoding processing at the time of

the data reproduction processing in the Information Storage Division playback equipment of this invention.
[Drawing 23]It is a figure showing the example of composition of the RIBOKESHON table used in the Information Storage Division playback equipment of this invention.
[Drawing 24]It is a figure explaining the processing in the case of carrying out application ** of the EKB distribution tree in the Information Storage Division playback equipment of this invention at the inspection of a RIBOKU device.
[Drawing 25]It is a figure showing the example of a format of applicable validation key blocks (EKB) in the Information Storage Division playback equipment of this invention.
[Drawing 26]It is a figure explaining the composition of the tag of validation key blocks (EKB).
[Drawing 27]It is a figure (Example 1) explaining the EKB tracking processing for a RIBOKU entity judging.
[Drawing 28]It is a figure (Example 2) explaining the EKB tracking processing for a RIBOKU entity judging.
[Drawing 29]It is a flow chart explaining the EKB tracking processing for a RIBOKU entity judging.
[Drawing 30]It is a flow chart explaining the processing which verifies a signature in the Information Storage Division playback equipment of this inventionand performs data reproduction.
[Drawing 31]It is a flow chart explaining the processing which verifies the signature to enciphered content in the Information Storage Division playback equipment of this inventionand performs data reproduction.
[Drawing 32]It is a flow chart explaining the processing which verifies the signature to a title key in the Information Storage Division playback equipment of this inventionand performs data reproduction.
[Drawing 33]It is a flow chart explaining the copy control processing at the time of the Data Recording Sub-Division processing in the Information Storage Division playback equipment of this invention.
[Drawing 34]It is a flow chart explaining the copy control processing at the time of the data reproduction processing in the Information Storage Division playback equipment of this invention.
[Drawing 35]In the Information Storage Division playback equipment of this inventionit is a block diagram showing the processing means composition in the case of performing data processing with software.
[Description of Notations]
100 Recording and reproducing device
110 Bus
120 Input-and-output I/F
130 MPEG codec
140 Input-and-output I/F
141 A/Da D/A converter

150 Cipher-processing means
160 ROM
170 CPU
180 Memory
190 Drive
200 Recording medium
210 Recording-medium I/F
300 TS processing means
600607 Terminal
602 Bit stream purser
603 PLL
604 Time stamp generation circuit
605 Block seed additional circuit
606 Smoothing buffer
800806 Terminal
801 Block seed separation circuits
802 Output controlling circuit
803 Comparator
804 Timing generating circuit
805 27 MHz clocks
901904913 Terminal
902 MPEG video encoder
903 Video stream buffer
905 MPEG audio encoder
906 Audio stream buffer
908 Multiplexing scheduler
909 Transport packet coding equipment
910 Arrival-time-stamps calculating means
911 Block seed additional circuit
912 Smoothing buffer
976 Switch
1001 Version
1002 Depth
1003 Data pointer
1004 Tag pointer
1005 Signature pointer
1006 Data division
1007 Tag part
1008 Signature
2001 Bus
2002 CPU
2003 ROM
2004 RAM
2005 Hard disk

2006 Outputting part
2007 Input part
2008 Communications department
2009 Drive
2010 Removable recording medium
2011 Input/output interface

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－236622
（P2002－236622A）
(43)公開日　平成14年８月23日(2002.8.23)

| (51)Int.Cl.[7] | 識別記号 | ＦＩ | | テーマコード（参考） |
|---|---|---|---|---|
| Ｇ０６Ｆ　12/14 | ３２０ | Ｇ０６Ｆ　12/14 | ３２０Ｅ | ５Ｂ０１７ |
| | | | ３２０Ｆ | ５Ｊ１０４ |
| Ｇ０９Ｃ　1/00 | ６４０ | Ｇ０９Ｃ　1/00 | ６４０Ｂ | |
| Ｈ０４Ｌ　9/32 | | Ｈ０４Ｌ　9/00 | ６７５Ｂ | |

審査請求　未請求　請求項の数24　ＯＬ　（全 42 頁）

(21)出願番号　特願2001－34969(P2001－34969)

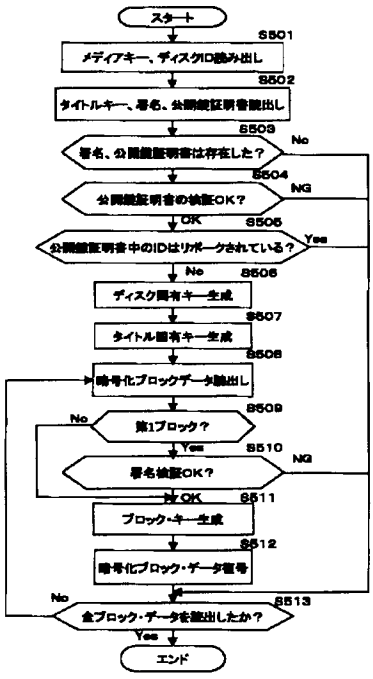
(22)出願日　平成13年２月13日(2001.2.13)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　浅野　智之
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100101801
弁理士　山田　英治　（外２名）

Ｆターム(参考)　5B017 AA06 BA07 BA09 CA09
5J104 AA01 AA09 AA16 EA02 EA04
EA26 LA03 LA06 NA02 NA05
PA14

(54)【発明の名称】　情報再生装置、情報記録装置、情報再生方法、情報記録方法、および情報記録媒体、並びにプログラム記憶媒体

(57)【要約】
【課題】　コンテンツ再生において、正当な記録コンテンツ記録であるか否かを判定して再生する構成を持つ情報記録再生装置および方法を提供する。
【解決手段】　データを情報記録媒体に記録する際にデジタル署名および公開鍵証明書を記録し、コンテンツを記録した記録装置を特定可能とした。不正に記録されたデータを含む記録媒体が流通しても、記録装置を特定しシステムからの排除が行える。情報再生装置は、データを読み出す際に署名および公開鍵証明書の正当性を確認し、コンテンツ記録者を特定し、公開鍵証明書、デジタル署名の改竄の無いことを確認した後にデータを再生する。本構成により、不正な記録装置による記録コンテンツの利用（再生）の効率的排除が可能となる。



【特許請求の範囲】
【請求項１】記録媒体から情報を再生する情報再生装置において、
前記記録媒体に格納された暗号化コンテンツ記録主体の公開鍵証明書の検証処理を実行し、正当性の確認された公開鍵証明書から前記コンテンツ記録主体の公開鍵を取得して、該取得した公開鍵に基づいて、コンテンツ記録主体のデジタル署名の検証処理を実行し、該検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行することを特徴とする情報再生装置。
【請求項２】前記暗号処理手段は、
前記記録媒体に格納された暗号化コンテンツのコンテンツを署名対象として生成されたコンテンツ記録主体のデジタル署名の検証処理を実行し、該検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行する構成であることを特徴とする請求項１に記載の情報再生装置。
【請求項３】前記暗号処理手段は、
前記記録媒体に格納された暗号化コンテンツに対応して設定されるタイトルキーを署名対象として生成されたコンテンツ記録主体のデジタル署名の検証処理を実行し、該検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行する構成であることを特徴とする請求項１に記載の情報再生装置。
【請求項４】前記情報再生装置は、
複数の異なる情報再生装置をリーフとした階層キーツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、
前記暗号処理手段は、
前記情報再生装置に内蔵したキーに基づいてキーツリーのパス上の下位キーによる上位キーの暗号化処理データからなる有効化キーブロック（ＥＫＢ）の復号を実行して前記記録媒体に格納された暗号データの復号処理に必要な復号キー生成用データを取得する構成を有することを特徴とする請求項１に記載の情報再生装置。
【請求項５】前記復号キー生成用データは、複数の情報再生装置において共通なマスターキー、または記録媒体に固有のメディアキーであることを特徴とする請求項４に記載の情報再生装置。
【請求項６】記録媒体に対して情報を記録する情報記録装置において、
記録媒体に格納するコンテンツの暗号化処理を実行する暗号処理手段を有し、
該暗号処理手段は、前記格納コンテンツの記録主体のデジタル署名を生成し、暗号化コンテンツ、デジタル署名および、暗号化コンテンツ記録主体の公開鍵証明書を対応付けて記録媒体に格納する処理を実行する構成を有することを特徴とする情報記録装置。
【請求項７】前記情報記録装置は、
格納コンテンツ、デジタル署名、公開鍵証明書のアドレスを対応付けた管理テーブルを生成し、前記記録媒体に格納する処理を実行する構成を有することを特徴とする請求項６に記載の情報記録装置。
【請求項８】前記暗号処理手段は、
前記記録媒体に格納する暗号化コンテンツのコンテンツを署名対象としてコンテンツ記録主体のデジタル署名の生成処理を実行し、生成した署名を格納コンテンツに対応付けて格納する構成であることを特徴とする請求項６に記載の情報記録装置。
【請求項９】前記暗号処理手段は、
前記記録媒体に格納する暗号化コンテンツに対応して設定されるタイトルキーを署名対象としてコンテンツ記録主体のデジタル署名の生成処理を実行し、生成した署名を格納コンテンツに対応付けて格納する構成であることを特徴とする請求項６に記載の情報記録装置。
【請求項１０】前記情報記録装置は、
複数の異なる情報記録装置をリーフとした階層キーツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、前記暗号処理手段は、
前記情報記録装置に内蔵したキーに基づいてキーツリーのパス上の下位キーによる上位キーの暗号化処理データからなる有効化キーブロック（ＥＫＢ）の復号を実行して前記記録媒体に格納するデータの暗号化処理に必要な暗号化キー生成用データを取得する構成を有することを特徴とする請求項６に記載の情報記録装置。
【請求項１１】前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキー、または記録媒体に固有のメディアキーであることを特徴とする請求項１０に記載の情報記録装置。
【請求項１２】記録媒体から情報を再生する情報再生方法において、
前記記録媒体に格納された暗号化コンテンツ記録主体の公開鍵証明書の検証処理を実行する公開鍵証明書検証ステップと、
正当性の確認された公開鍵証明書から前記コンテンツ記録主体の公開鍵を取得して、該取得した公開鍵に基づいて、コンテンツ記録主体のデジタル署名の検証処理を実行する署名検証ステップと、
該署名検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行するステップと、
を有することを特徴とする情報再生方法。
【請求項１３】前記情報再生方法における前記署名検証ステップは、
前記記録媒体に格納された暗号化コンテンツのコンテンツを署名対象として生成されたコンテンツ記録主体のデジタル署名の検証処理を実行するステップを含み、該検証の結果、署名の正当性が確認されたことを条件として

暗号化コンテンツの復号処理を実行することを特徴とする請求項１２に記載の情報再生方法。
【請求項１４】前記情報再生方法における前記署名検証ステップは、
前記記録媒体に格納された暗号化コンテンツに対応して設定されるタイトルキーを署名対象として生成されたコンテンツ記録主体のデジタル署名の検証処理を実行するステップを含み、該検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行することを特徴とする請求項１２に記載の情報再生方法。
【請求項１５】前記情報再生方法は、さらに、
複数の異なる情報再生装置をリーフとした階層キーツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーに基づいて、有効化キーブロック（ＥＫＢ）の復号を実行して前記記録媒体に格納された暗号データの復号処理に必要な復号キー生成用データを取得する処理を実行することを特徴とする請求項１２に記載の情報再生方法。
【請求項１６】記録媒体に対して情報を記録する情報記録方法において、
記録媒体に格納するコンテンツの暗号化処理を実行する暗号処理ステップと、前記格納コンテンツの記録主体のデジタル署名を生成するステップと、
暗号化コンテンツ、デジタル署名および、暗号化コンテンツ記録主体の公開鍵証明書を対応付けて記録媒体に格納するステップと、を有することを特徴とする情報記録方法。
【請求項１７】前記情報記録方法は、さらに、
格納コンテンツ、デジタル署名、公開鍵証明書のアドレスを対応付けた管理テーブルを生成し、前記記録媒体に格納する処理を実行することを特徴とする請求項１６に記載の情報記録方法。
【請求項１８】前記情報記録方法は、さらに、
前記記録媒体に格納する暗号化コンテンツのコンテンツを署名対象としてコンテンツ記録主体のデジタル署名の生成処理を実行し、生成した署名を格納コンテンツに対応付けて格納することを特徴とする請求項１６に記載の情報記録方法。
【請求項１９】前記情報記録方法は、さらに、
前記記録媒体に格納する暗号化コンテンツに対応して設定されるタイトルキーを署名対象としてコンテンツ記録主体のデジタル署名の生成処理を実行し、生成した署名を格納コンテンツに対応付けて格納することを特徴とする請求項１６に記載の情報記録方法。
【請求項２０】前記情報記録方法は、さらに、
前記情報記録装置に内蔵した複数の異なる情報記録装置をリーフとした階層キーツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーに基づいて有効化キーブロック（ＥＫＢ）の復号を実行して前記記録媒体に格納するデータの暗号化処理に必要な暗号化キー生成用データを取得する処理を実行することを特徴とする請求項１６に記載の情報記録方法。
【請求項２１】暗号化コンテンツを格納した情報記録媒体であり、
該暗号化コンテンツを記録した記録主体の識別データと、
前記記録主体の公開鍵証明書と、
前記記録主体のデジタル署名とを格納したことを特徴とする情報記録媒体。
【請求項２２】前記情報記録媒体は、さらに、
格納コンテンツ、デジタル署名、公開鍵証明書のアドレスを対応付けた管理テーブルを格納したことを特徴とする請求項２１に記載の情報記録媒体。
【請求項２３】記録媒体から情報を再生する情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを格納したプログラム記憶媒体であって、前記コンピュータ・プログラムは、
前記記録媒体に格納された暗号化コンテンツ記録主体の公開鍵証明書の検証処理を実行する公開鍵証明書検証ステップと、
正当性の確認された公開鍵証明書から前記コンテンツ記録主体の公開鍵を取得して、該取得した公開鍵に基づいて、コンテンツ記録主体のデジタル署名の検証処理を実行する署名検証ステップと、
該署名検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行するステップと、
を有することを特徴とするプログラム記憶媒体。
【請求項２４】記録媒体に対して情報を記録する情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを格納したプログラム記憶媒体であって、前記コンピュータ・プログラムは、
記録媒体に格納するコンテンツの暗号化処理を実行する暗号処理ステップと、
前記格納コンテンツの記録主体のデジタル署名を生成するステップと、
暗号化コンテンツ、デジタル署名および、暗号化コンテンツ記録主体の公開鍵証明書を対応付けて記録媒体に格納するステップと、
を有することを特徴とするプログラム記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、情報再生装置、情報記録装置、情報再生方法、情報記録方法、および情報記録媒体、並びにプログラム記憶媒体に関し、特に、情報記録装置がデータを情報記録媒体に記録する際に自身のデジタル署名および公開鍵証明書をデータと共に記録し、情報再生装置がデータを読み出す際に上記デジタル署名および公開鍵証明書の正当性を確認し、また情報記

録装置がリボークされていないことを確認した後にデータを読み出す構成とした情報再生装置、情報記録装置、情報再生方法、情報記録方法、および情報記録媒体、並びにプログラム記憶媒体に関する。

【０００２】

【従来の技術】デジタル信号処理技術の進歩、発展に伴い、近年においては、情報を、デジタル的に記録する記録装置や記録媒体が普及しつつある。このようなデジタル記録装置および記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにデジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができるため、コピーが違法に行われた記録媒体が市場に流通することになると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。昨今では、このようなデジタルデータの不正なコピーを防ぐため、デジタル記録装置および記録媒体に違法なコピーを防止するための様々な仕組み（システム）が導入されている。

【０００３】例えば、ＭＤ（ミニディスク）（ＭＤは商標）装置において、違法なコピーを防止する方法として、ＳＣＭＳ(Serial Copy Management System)が採用されている。ＳＣＭＳは、データ再生側において、オーディオデータとともにＳＣＭＳ信号をデジタルインタフェース（ＤＩＦ）から出力し、データ記録側において、再生側からのＳＣＭＳ信号に基づいて、再生側からのオーディオデータの記録を制御することにより違法なコピーを防止するシステムである。

【０００４】具体的にはＳＣＭＳ信号は、オーディオデータが、何度でもコピーが許容されるコピーフリー（copy free）のデータであるか、１度だけコピーが許されている（copy once allowed）データであるか、またはコピーが禁止されている（copy prohibited）データであるかを表す信号である。データ記録側において、ＤＩＦからオーディオデータを受信すると、そのオーディオデータとともに送信されるＳＣＭＳ信号を検出する。そして、ＳＣＭＳ信号が、コピーフリー（copy free）となっている場合には、オーディオデータをＳＣＭＳ信号とともにミニディスクに記録する。また、ＳＣＭＳ信号が、コピーを１度のみ許可（copy once allowed）となっている場合には、ＳＣＭＳ信号をコピー禁止（copy prohibited）に変更して、オーディオデータとともに、ミニディスクに記録する。さらに、ＳＣＭＳ信号が、コピー禁止（copy prohibited）となっている場合には、オーディオデータの記録を行わない。このようなＳＣＭＳを使用した制御を行なうことで、ミニディスク装置では、ＳＣＭＳによって、著作権を有するオーディオデータが、違法にコピーされるのを防止するようになっている。

【０００５】しかしながら、ＳＣＭＳは上述のようにＳＣＭＳ信号に基づいて再生側からのオーディオデータの記録を制御する構成をデータを記録する機器自体が有していることが前提であるため、ＳＣＭＳの制御を実行する構成を持たないミニディスク装置が製造された場合には、対処するのが困難となる。そこで、例えば、ＤＶＤプレーヤでは、コンテンツ・スクランブルシステムを採用することにより、著作権を有するデータの違法コピーを防止する構成となっている。

【０００６】コンテンツ・スクランブルシステムでは、ＤＶＤ－ＲＯＭ(Read Only Memory)に、ビデオデータやオーディオデータ等が暗号化されて記録されており、その暗号化されたデータを復号するのに用いるキー（復号鍵）が、ライセンスを受けたＤＶＤプレーヤに与えられる。ライセンスは、不正コピーを行わない等の所定の動作規定に従うように設計されたＤＶＤプレーヤに対して与えられる。従って、ライセンスを受けたＤＶＤプレーヤでは、与えられたキーを利用して、ＤＶＤ－ＲＯＭに記録された暗号化データを復号することにより、ＤＶＤ－ＲＯＭから画像や音声を再生することができる。

【０００７】一方、ライセンスを受けていないＤＶＤプレーヤは、暗号化されたデータを復号するためのキーを有していないため、ＤＶＤ－ＲＯＭに記録された暗号化データの復号を行うことができない。このように、コンテンツ・スクランブルシステム構成では、ライセンス時に要求される条件を満たしていないＤＶＤプレーヤは、デジタルデータを記録したＤＶＤ－ＲＯＭの再生を行なえないことになり、不正コピーが防止されるようになっている。

【０００８】しかしながら、ＤＶＤ－ＲＯＭで採用されているコンテンツ・スクランブルシステムは、ユーザによるデータの書き込みが不可能な記録媒体（以下、適宜、ＲＯＭメディアという）を対象としており、ユーザによるデータの書き込みが可能な記録媒体（以下、適宜、ＲＡＭメディアという）への適用については考慮されていない。

【０００９】即ち、ＲＯＭメディアに記録されたデータが暗号化されていても、その暗号化されたデータを、そのまま全部、ＲＡＭメディアにコピーした場合には、ライセンスを受けた正当な装置で再生可能な、いわゆる海賊版を作成することができてしまう。

【００１０】そこで、本出願人は、先の特許出願、特開平１１－２２４４６１号公報（特願平１０－２５３１０号）において、個々の記録媒体を識別する為の情報（以下、媒体識別情報と記述する）を、他のデータとともに記録媒体に記録し、この媒体識別情報のライセンスを受けた装置であることを条件として、その条件が満たされた場合にのみ記録媒体の媒体識別情報へのアクセスが可能となる構成を提案した。

【００１１】この方法では、記録媒体上のデータは、媒体識別情報とライセンスを受けることにより得られる秘

密キー（マスターキー）により暗号化され、ライセンスを受けていない装置が、この暗号化されたデータを読み出したとしても、意味のあるデータを得ることができないようになっている。なお、装置はライセンスを受ける際、不正な複製（違法コピー）ができないように、その動作が規定される。

【００１２】ライセンスを受けていない装置は、媒体識別情報にアクセスできず、また、媒体識別情報は個々の媒体毎に個別の値となっているため、ライセンスを受けていない装置が、記録媒体に記録されている、暗号化されたデータのすべてを新たな記録媒体に複製したとしても、そのようにして作成された記録媒体に記録されたデータは、ライセンスを受けていない装置は勿論、ライセンスを受けた装置においても、正しく復号することができないから、実質的に、違法コピーが防止されることになる。

【００１３】ところで、上記の構成においては、ライセンスを受けた装置において格納されるマスターキーは全機器において共通であるのが一般的である。このように複数の機器に対して共通のマスターキーを格納するのは、１つの機器で記録された媒体を他の機器で再生可能とする（インターオペラビリティを確保する）ために必要な条件であるからである。

【００１４】しかし、この方式においては、攻撃者が１つの機器の攻撃に成功し、マスターキーを取出した場合、全システムにおいて暗号化されて記録されているデータを復号することができてしまい、システム全体が崩壊する。これを防ぐためには、ある機器が攻撃されてマスターキーが露呈したことが発覚した場合、マスターキーを新たなものに更新し、攻撃に屈した機器以外の全機器に新たに更新されたマスターキーを与えることが必要になる。この構成を実現する一番単純な方式としては、個々の機器に固有の鍵（デバイスキー）を与えておき、新たなマスターキーを個々のデバイスキーで暗号化した値を用意し、記録媒体を介して機器に伝送する方式が考えられるが、機器の台数に比例して伝送すべき全メッセージ量が増加するという問題がある。

【００１５】上記問題を解決する構成として、本出願人は、各情報記録再生装置をｎ分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体もしくは通信回線を介して、コンテンツデータの記録媒体への記録もしくは記録媒体からの再生に必要な鍵（マスターキーもしくはメディアキー）を配信し、これを用いて各装置がコンテンツデータの記録、再生を行うようにすることにより、正当な（秘密が露呈していない装置に）対して少ないメッセージ量でマスターキーもしくはメディアキーを伝送できる構成を、先に提案し、すでに特許出願（特願平２０００－１０５３２８）している。具体的には、記録媒体への記録もしくは記録媒体からの再生に必要な鍵を生成するために必要となるキー、例えばｎ分木の各葉（リーフ）を構成するノードに割り当てたノードキーを更新ノードキーとして設定し、更新ノードキーを正当な機器のみが有するリーフキー、ノードキーで復号可能な態様で暗号化処理した情報を含む有効化キーブロック（ＥＫＢ）を各情報記録再生装置に配信し、有効化キーブロック（ＥＫＢ）を受信した各情報記録再生装置のＥＫＢ復号処理により、各装置が記録もしくは記録媒体からの再生に必要な鍵を取得可能とした構成である。

【００１６】

【発明が解決しようとする課題】上記の構成においては、秘密が露呈した装置をシステムから排除することは可能であるが、このためにはどの装置の秘密が露呈したかを特定する必要がある。たとえば、ある装置から盗んだ秘密を搭載したクローンデバイスが作られ、ブラックマーケットで販売されていたことが特定できれば、秘密を盗まれた装置が特定され、システムから排除されることになる。

【００１７】ところで、システムに対する攻撃を考えると、上記のようにクローンデバイスが作られて出まわるのではなく、ある情報記録装置を改造して、たとえば本来は暗号化して記録すべきデータを平文で記録するなどの、不正な記録を行わせて、その結果作られた、不正に記録されたデータを含む記録媒体を販売するなどの行為が考えられる。この場合、その記録媒体にデータを不正に記録した装置が特定できれば、それをシステムから排除し、新しいコンテンツデータをその装置では復号させないように配信することが、上記の方法で可能である。

【００１８】本発明は、上述の問題を解決するものであり、情報記録装置がデータを情報記録媒体に記録する際に自身のデジタル署名および公開鍵証明書をデータと共に記録し、情報再生装置がデータを読み出す際に上記デジタル署名および公開鍵証明書の正当性を確認した後にデータを読み出す構成とすることにより、コンテンツ記録が正当に行われたものであることを条件として再生を可能とするシステムを提供することを目的とする。

【００１９】

【課題を解決するための手段】本発明の第1の側面は、記録媒体から情報を再生する情報再生装置において、前記記録媒体に格納された暗号化コンテンツ記録主体の公開鍵証明書の検証処理を実行し、正当性の確認された公開鍵証明書から前記コンテンツ記録主体の公開鍵を取得して、該取得した公開鍵に基づいて、コンテンツ記録主体のデジタル署名の検証処理を実行し、該検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行することを特徴とする情報再生装置にある。

【００２０】さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記記録媒体に格納された暗号化コンテンツのコンテンツを署名対象として生成されたコンテンツ記録主体のデジタル署名の検証処

理を実行し、該検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行する構成であることを特徴とする。

【００２１】さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記記録媒体に格納された暗号化コンテンツに対応して設定されるタイトルキーを署名対象として生成されたコンテンツ記録主体のデジタル署名の検証処理を実行し、該検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行する構成であることを特徴とする。

【００２２】さらに、本発明の情報再生装置の一実施態様において、前記情報再生装置は、複数の異なる情報再生装置をリーフとした階層キーツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、前記暗号処理手段は、前記情報再生装置に内蔵したキーに基づいてキーツリーのパス上の下位キーによる上位キーの暗号化処理データからなる有効化キーブロック（ＥＫＢ）の復号を実行して前記記録媒体に格納された暗号データの復号処理に必要な復号キー生成用データを取得する構成を有することを特徴とする。

【００２３】さらに、本発明の情報再生装置の一実施態様において、前記復号キー生成用データは、複数の情報再生装置において共通なマスターキー、または記録媒体に固有のメディアキーであることを特徴とする。

【００２４】さらに、本発明の第２の側面は、記録媒体に対して情報を記録する情報記録装置において、記録媒体に格納するコンテンツの暗号化処理を実行する暗号処理手段を有し、該暗号処理手段は、前記格納コンテンツの記録主体のデジタル署名を生成し、暗号化コンテンツ、デジタル署名および、暗号化コンテンツ記録主体の公開鍵証明書を対応付けて記録媒体に格納する処理を実行する構成を有することを特徴とする情報記録装置にある。

【００２５】さらに、本発明の情報記録装置の一実施態様において、前記情報記録装置は、格納コンテンツ、デジタル署名、公開鍵証明書のアドレスを対応付けた管理テーブルを生成し、前記記録媒体に格納する処理を実行する構成を有することを特徴とする。

【００２６】さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記記録媒体に格納する暗号化コンテンツのコンテンツを署名対象としてコンテンツ記録主体のデジタル署名の生成処理を実行し、生成した署名を格納コンテンツに対応付けて格納する構成であることを特徴とする。

【００２７】さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記記録媒体に格納する暗号化コンテンツに対応して設定されるタイトルキーを署名対象としてコンテンツ記録主体のデジタル署名の生成処理を実行し、生成した署名を格納コンテンツに対応付けて格納する構成であることを特徴とする。

【００２８】さらに、本発明の情報記録装置の一実施態様において、前記情報記録装置は、複数の異なる情報記録装置をリーフとした階層キーツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、前記暗号処理手段は、前記情報記録装置に内蔵したキーに基づいてキーツリーのパス上の下位キーによる上位キーの暗号化処理データからなる有効化キーブロック（ＥＫＢ）の復号を実行して前記記録媒体に格納するデータの暗号化処理に必要な暗号化キー生成用データを取得する構成を有することを特徴とする。

【００２９】さらに、本発明の情報記録装置の一実施態様において、前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキー、または記録媒体に固有のメディアキーであることを特徴とする。

【００３０】さらに、本発明の第３の側面は、記録媒体から情報を再生する情報再生方法において、前記記録媒体に格納された暗号化コンテンツ記録主体の公開鍵証明書の検証処理を実行する公開鍵証明書検証ステップと、正当性の確認された公開鍵証明書から前記コンテンツ記録主体の公開鍵を取得して、該取得した公開鍵に基づいて、コンテンツ記録主体のデジタル署名の検証処理を実行する署名検証ステップと、該署名検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行するステップと、を有することを特徴とする情報再生方法にある。

【００３１】さらに、本発明の情報再生方法の一実施態様において、前記情報再生方法における前記署名検証ステップは、前記記録媒体に格納された暗号化コンテンツのコンテンツを署名対象として生成されたコンテンツ記録主体のデジタル署名の検証処理を実行するステップを含み、該検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行することを特徴とする。

【００３２】さらに、本発明の情報再生方法の一実施態様において、前記情報再生方法における前記署名検証ステップは、前記記録媒体に格納された暗号化コンテンツに対応して設定されるタイトルキーを署名対象として生成されたコンテンツ記録主体のデジタル署名の検証処理を実行するステップを含み、該検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行することを特徴とする。

【００３３】さらに、本発明の情報再生方法の一実施態様において、前記情報再生方法は、さらに、複数の異なる情報再生装置をリーフとした階層キーツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーに基づいて、有効化キーブロック（ＥＫＢ）の復号を実行して前記記録媒体に格納された暗号データの復号処理に必要な復号キー生成用データを取得する処理を実行することを特徴とする。

【００３４】さらに、本発明の第４の側面は、記録媒体に対して情報を記録する情報記録方法において、記録媒体に格納するコンテンツの暗号化処理を実行する暗号処理ステップと、前記格納コンテンツの記録主体のデジタル署名を生成するステップと、暗号化コンテンツ、デジタル署名および、暗号化コンテンツ記録主体の公開鍵証明書を対応付けて記録媒体に格納するステップと、を有することを特徴とする情報記録方法にある。

【００３５】さらに、本発明の情報記録方法の一実施態様において、前記情報記録方法は、さらに、格納コンテンツ、デジタル署名、公開鍵証明書のアドレスを対応付けた管理テーブルを生成し、前記記録媒体に格納する処理を実行することを特徴とする。

【００３６】さらに、本発明の情報記録方法の一実施態様において、前記情報記録方法は、さらに、前記記録媒体に格納する暗号化コンテンツのコンテンツを署名対象としてコンテンツ記録主体のデジタル署名の生成処理を実行し、生成した署名を格納コンテンツに対応付けて格納することを特徴とする。

【００３７】さらに、本発明の情報記録方法の一実施態様において、前記情報記録方法は、さらに、前記記録媒体に格納する暗号化コンテンツに対応して設定されるタイトルキーを署名対象としてコンテンツ記録主体のデジタル署名の生成処理を実行し、生成した署名を格納コンテンツに対応付けて格納することを特徴とする。

【００３８】さらに、本発明の情報記録方法の一実施態様において、前記情報記録方法は、さらに、前記情報記録装置に内蔵した複数の異なる情報記録装置をリーフとした階層キーツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーに基づいて有効化キーブロック（ＥＫＢ）の復号を実行して前記記録媒体に格納するデータの暗号化処理に必要な暗号化キー生成用データを取得する処理を実行することを特徴とする。

【００３９】さらに、本発明の第５の側面は、暗号化コンテンツを格納した情報記録媒体であり、該暗号化コンテンツを記録した記録主体の識別データと、前記記録主体の公開鍵証明書と、前記記録主体のデジタル署名とを格納したことを特徴とする情報記録媒体にある。

【００４０】さらに、本発明の情報記録媒体の一実施態様において、前記情報記録媒体は、さらに、格納コンテンツ、デジタル署名、公開鍵証明書のアドレスを対応付けた管理テーブルを格納したことを特徴とする。

【００４１】さらに、本発明の第６の側面は、記録媒体から情報を再生する情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを格納したプログラム記憶媒体であって、前記コンピュータ・プログラムは、前記記録媒体に格納された暗号化コンテンツ記録主体の公開鍵証明書の検証処理を実行する公開鍵証明書検証ステップと、正当性の確認された公開鍵証明書から前記コンテンツ記録主体の公開鍵を取得して、該取得した公開鍵に基づいて、コンテンツ記録主体のデジタル署名の検証処理を実行する署名検証ステップと、該署名検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行するステップと、を有することを特徴とするプログラム記憶媒体にある。

【００４２】さらに、本発明の第７の側面は、記録媒体に対して情報を記録する情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを格納したプログラム記憶媒体であって、前記コンピュータ・プログラムは、記録媒体に格納するコンテンツの暗号化処理を実行する暗号処理ステップと、前記格納コンテンツの記録主体のデジタル署名を生成するステップと、暗号化コンテンツ、デジタル署名および、暗号化コンテンツ記録主体の公開鍵証明書を対応付けて記録媒体に格納するステップと、を有することを特徴とするプログラム記憶媒体にある。

【００４３】

【作用】本発明においては、情報記録装置がデータを情報記録媒体に記録する際に自身のデジタル署名および公開鍵証明書をデータと共に記録するようにした。このことにより、情報を記録する際には、必ず、どの記録装置が記録したかという証拠もデータと共に記録するようにしているので、もし不正に記録されたデータを含む記録媒体が流通したとしても、それをどの記録装置が記録したか特定できるので、システムからの排除が行える。

【００４４】さらに、情報再生装置がデータを読み出す際に上記デジタル署名および公開鍵証明書の正当性を確認した後にデータを読み出す構成とした。このことにより、不正な記録装置が、不正な記録データに対してデジタル署名を記録しないような攻撃を無力なものにしている。すなわち、記録されたデータに対して有効なデジタル署名がなければ、正当な再生装置はそのデータを再生しないからである。

【００４５】

【発明の実施の形態】［システム構成］図１は、本発明を適用した記録再生装置１００の一実施例構成を示すブロック図である。記録再生装置１００は、入出力Ｉ／Ｆ(Interface)１２０、ＭＰＥＧ(Moving Picture Experts Group)コーデック１３０、Ａ／Ｄ，Ｄ／Ａコンバータ１４１を備えた入出力Ｉ／Ｆ(Interface)１４０、暗号処理手段１５０、ＲＯＭ（Read Only Memory）１６０、ＣＰＵ(Central Processing Unit)１７０、メモリ１８０、記録媒体２００の記録媒体インタフェース（Ｉ／Ｆ）１９０、さらにトランスポート・ストリーム処理手段（ＴＳ処理手段）３００を有し、これらはバス１１０によって相互に接続されている。

【００４６】入出力Ｉ／Ｆ１２０は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成す

るデジタル信号を受信し、バス１１０上に出力するとともに、バス１１０上のデジタル信号を受信し、外部に出力する。ＭＰＥＧコーデック１３０は、バス１１０を介して供給されるＭＰＥＧ符号化されたデータを、ＭＰＥＧデコードし、入出力Ｉ／Ｆ１４０に出力するとともに、入出力Ｉ／Ｆ１４０から供給されるデジタル信号をＭＰＥＧエンコードしてバス１１０上に出力する。入出力Ｉ／Ｆ１４０は、Ａ／Ｄ，Ｄ／Ａコンバータ１４１を内蔵している。入出力Ｉ／Ｆ１４０は、外部から供給されるコンテンツとしてのアナログ信号を受信し、Ａ／Ｄ，Ｄ／Ａコンバータ１４１でＡ／Ｄ(Analog Digital)変換することで、デジタル信号として、ＭＰＥＧコーデック１３０に出力するとともに、ＭＰＥＧコーデック１３０からのデジタル信号を、Ａ／Ｄ，Ｄ／Ａコンバータ１４１でＤ／Ａ(Digital Analog)変換することで、アナログ信号として、外部に出力する。

【００４７】暗号処理手段１５０は、例えば、１チップのＬＳＩ(Large Scale IntegratedCurcuit)で構成され、バス１１０を介して供給されるコンテンツとしてのデジタル信号を暗号化し、または復号し、バス１１０上に出力する構成を持つ。なお、暗号処理手段１５０は１チップＬＳＩに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構成による処理手段としての構成については後段で説明する。

【００４８】ＲＯＭ１６０は、例えば、記録再生装置ごとに固有の、あるいは複数の記録再生装置のグループごとに固有のデバイスキーであるリーフキーと、複数の記録再生装置、あるいは複数のグループに共有のデバイスキーであるノードキーを記憶している。さらに、記録再生装置固有の、公開鍵暗号系の秘密鍵と、公開鍵証明書、さらに、信頼できるセンタの公開鍵を記憶しておく。

【００４９】ここで、公開鍵証明書は、図２に示すように、その証明書利用者、例えば記録再生装置のＩＤと、利用者の公開鍵を格納し、その他のデータをメッセージとして信頼できるセンタ（認証局）がデジタル署名を施したデータである。センタのデジタル署名の検証処理を、予め取得済みのセンタの公開鍵を用いて実行して公開鍵証明書の正当性が確認でき、格納された公開鍵を取り出して利用することができる。

【００５０】ＣＰＵ１７０は、メモリ１８０に記憶されたプログラムを実行することで、ＭＰＥＧコーデック１３０や暗号処理手段１５０等を制御する。メモリ１８０は、例えば、不揮発性メモリで、ＣＰＵ１７０が実行するプログラムや、ＣＰＵ１７０の動作上必要なデータを記憶する。記録媒体インタフェース１９０は、デジタルデータを記録再生可能な記録媒体２００を駆動することにより、記録媒体２００からデジタルデータを読み出し（再生し）、バス１１０上に出力するとともに、バス１１０を介して供給されるデジタルデータを、記録媒体２００に供給して記録させる。また、プログラムをＲＯＭ１６０に、デバイスキー等をメモリ１８０に記憶する構成としてもよい。

【００５１】記録媒体２００は、例えば、ＤＶＤ、ＣＤ等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはＲＡＭ等の半導体メモリ等のデジタルデータの記憶可能な媒体であり、本実施の形態では、記録媒体インタフェース１９０に対して着脱可能な構成であるとする。但し、記録媒体２００は、記録再生装置１００に内蔵する構成としてもよい。

【００５２】トランスポート・ストリーム処理手段（ＴＳ処理手段）３００は、後段において図を用いて詳細に説明するが、例えば複数のＴＶプログラム（コンテンツ）が多重化されたトランスポートストリームから特定のプログラム（コンテンツ）に対応するトランスポートパケットを取り出して、取り出したトランスポートストリームの出現タイミング情報を各パケットとともに記録媒体２００に格納するためのデータ処理および、記録媒体２００からの再生処理時の出現タイミング制御処理を行なう。

【００５３】トランスポートストリームには、各トランスポートパケットの出現タイミング情報としてのＡＴＳ（Arrival Time Stamp：着信時刻スタンプ）が設定されており、このタイミングはＭＰＥＧ２システムズで規定されている仮想的なデコーダであるＴ－ＳＴＤ(Transport stream System Target Decoder)を破綻させないように符号化時に決定され、トランスポートストリームの再生時には、各トランスポートパケットに付加されたＡＴＳによって出現タイミングを制御する。トランスポート・ストリーム処理手段（ＴＳ処理手段）３００は、これらの制御を実行する。例えば、トランスポートパケットを記録媒体に記録する場合には、各パケットの間隔を詰めたソースパケットとして記録するが、各トランスポートパケットの出現タイミングを併せて記録媒体に保存することにより、再生時に各パケットの出力タイミングを制御することが可能となる。トランスポート・ストリーム処理手段（ＴＳ処理手段）３００は、ＤＶＤ等の記録媒体２００へのデータ記録時に、各トランスポートパケットの入力タイミングを表すＡＴＳ（ArrivalTime Stamp：着信時刻スタンプ）を付加して記録する。

【００５４】なお、本発明の処理システムにおいて処理されるデータはトランスポートストリームに従ったフォーマット・データに限られるものではない。従ってトランスポートストリーム以外のデータに関する処理を実行する場合は、図１に示すＴＳ処理手段は必ずしも必要とはならない。

【００５５】［データ記録処理およびデータ再生処理］次に、図１の記録再生装置における記録媒体に対するデータ記録処理および記録媒体からのデータ再生処理につ

いて、図３および図４のフローチャートを参照して説明する。外部からのデジタル信号のコンテンツを、記録媒体２００に記録する場合においては、図３（Ａ）のフローチャートにしたがった記録処理が行われる。即ち、デジタル信号のコンテンツ（デジタルコンテンツ）が、例えば、IEEE(Institute of Electrical and Electronics Engineers)1394シリアルバス等を介して、入出力Ｉ／Ｆ１２０に供給されると、ステップＳ１１において、入出力Ｉ／Ｆ１２０は、供給されるデジタルコンテンツを受信し、バス１１０を介して、ＴＳ処理手段３００または、暗号処理手段１５０に出力する。

【００５６】受信データがトランスポートストリーム処理を必要とする場合は、ＴＳ処理手段３００においてトランスポート・ストリーム処理が実行される。ＴＳ処理手段３００は、ステップＳ１２において、トランスポートストリームを構成する各トランスポートパケットにＡＴＳを付加したブロックデータを生成して、バス１１０を介して、暗号処理手段１５０に出力する。この処理については、さらに後段で詳細に説明する。

【００５７】暗号処理手段１５０は、ステップＳ１３において、受信したデジタルコンテンツに対する暗号化処理を実行し、その結果得られる暗号化コンテンツを、バス１１０を介して、記録媒体Ｉ／Ｆ１９０に出力する。暗号化コンテンツは、記録媒体Ｉ／Ｆ１９０を介して記録媒体２００に記録（Ｓ１４）され、記録処理を終了する。

【００５８】なお、IEEE1394シリアルバスを介して接続した装置相互間で、デジタルコンテンツを伝送するときの、デジタルコンテンツを保護するための規格として、本特許出願人であるソニー株式会社を含む５社によって、５ＣＤＴＣＰ(Five Company Digital Transmission Content Protection)（以下、適宜、ＤＴＣＰという）が定められているが、このＤＴＣＰでは、コピーフリーでないデジタルコンテンツを装置相互間で伝送する場合、データ伝送に先立って、送信側と受信側が、コピーを制御するためのコピー制御情報を正しく取り扱えるかどうかの認証を相互に行い、その後、送信側において、デジタルコンテンツを暗号化して伝送し、受信側において、その暗号化されたデジタルコンテンツ（暗号化コンテンツ）を復号するようになっている。

【００５９】このＤＴＣＰに規格に基づくデータ送受信においては、データ受信側の入出力Ｉ／Ｆ１２０は、ステップＳ１１で、IEEE1394シリアルバスを介して暗号化コンテンツを受信し、その暗号化コンテンツを、ＤＴＣＰに規格に準拠して復号し、平文のコンテンツとして、その後、暗号処理手段１５０に出力する。

【００６０】ＤＴＣＰによるデジタルコンテンツの暗号化は、時間変化するキーを生成し、そのキーを用いて行われる。暗号化されたデジタルコンテンツは、その暗号化に用いたキーを含めて、IEEE1394シリアルバス上を伝送され、受信側では、暗号化されたデジタルコンテンツを、そこに含まれるキーを用いて復号する。

【００６１】なお、ＤＴＣＰによれば、正確には、キーの初期値と、デジタルコンテンツの暗号化に用いるキーの変更タイミングを表すフラグとが、暗号化コンテンツに含められる。そして、受信側では、その暗号化コンテンツに含まれるキーの初期値を、やはり、その暗号化コンテンツに含まれるフラグのタイミングで変更していくことで、暗号化に用いられたキーが生成され、暗号化コンテンツが復号される。但し、ここでは、暗号化コンテンツに、その復号を行うためのキーが含まれていると等価であると考えても差し支えないため、以下では、そのように考えるものとする。ここで、ＤＴＣＰについては、例えば、http://www.dtcp.comのURL(Uniform Resource Locator)で特定されるＷｅｂページにおいて、インフォメイショナルバージョン(Informational Version)の取得が可能である。

【００６２】次に、外部からのアナログ信号のコンテンツを、記録媒体２００に記録する場合の処理について、図３（Ｂ）のフローチャートに従って説明する。アナログ信号のコンテンツ（アナログコンテンツ）が、入出力Ｉ／Ｆ１４０に供給されると、入出力Ｉ／Ｆ１４０は、ステップＳ２１において、そのアナログコンテンツを受信し、ステップＳ２２に進み、内蔵するＡ／Ｄ，Ｄ／Ａコンバータ１４１でＡ／Ｄ変換して、デジタル信号のコンテンツ（デジタルコンテンツ）とする。

【００６３】このデジタルコンテンツは、ＭＰＥＧコーデック１３０に供給され、ステップＳ２３において、ＭＰＥＧエンコード、すなわちＭＰＥＧ圧縮による符号化処理が実行され、バス１１０を介して、暗号処理手段１５０に供給される。

【００６４】以下、ステップＳ２４、Ｓ２５、Ｓ２６において、図３（Ａ）のステップＳ１２、Ｓ１３、Ｓ１４における処理と同様の処理が行われる。すなわち、必要であればＴＳ処理手段３００によるトランスポートパケットに対するＡＴＳ付加、暗号処理手段１５０における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体２００に記録して、記録処理を終了する。

【００６５】次に、記録媒体２００に記録されたコンテンツを再生して、デジタルコンテンツ、あるいはアナログコンテンツとして出力する処理について図４のフローに従って説明する。デジタルコンテンツとして外部に出力する処理は図４（Ａ）のフローチャートにしたがった再生処理として実行される。即ち、まず最初に、ステップＳ３１において、記録媒体Ｉ／Ｆ１９０によって、記録媒体２００に記録された暗号化コンテンツが読み出され、バス１１０を介して、暗号処理手段１５０に出力される。

【００６６】暗号処理手段１５０では、ステップＳ３２

において、記録媒体Ｉ／Ｆ１９０から供給される暗号化コンテンツが復号処理され、データがトランスポートストリームである場合は、復号データがバス１１０を介して、ＴＳ処理手段３００に出力され、ＴＳ処理が不要の場合は入出力Ｉ／Ｆ１２０に供給される。

【００６７】ＴＳ処理手段３００は、ステップＳ４３において、トランスポートストリームを構成する各トランスポートパケットのＡＴＳから出力タイミングを判定し、ＡＴＳに応じた制御を実行して、バス１１０を介して、入出力Ｉ／Ｆ１２０に供給する。入出力Ｉ／Ｆ１２０は、ＴＳ処理手段３００からのデジタルコンテンツを、外部に出力し、再生処理を終了する。なお、ＴＳ処理手段３００の処理、暗号処理手段１５０におけるデジタルコンテンツの復号処理については後述する。

【００６８】さらに、データは入出力Ｉ／Ｆ１２０に供給され、ステップＳ３４において、入出力Ｉ／Ｆ１２０はデジタルコンテンツを、外部に出力し、再生処理を終了する。

【００６９】なお、入出力Ｉ／Ｆ１２０は、ステップＳ３４で、IEEE1394シリアルバスを介してデジタルコンテンツを出力する場合には、ＤＴＣＰの規格に準拠して、上述したように、相手の装置との間で認証を相互に行い、その後、デジタルコンテンツを暗号化して伝送する。

【００７０】記録媒体２００に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図４（Ｂ）のフローチャートに従った再生処理が行われる。

【００７１】即ち、ステップＳ４１、Ｓ４２、Ｓ４３において、図４（Ａ）のステップＳ３１、Ｓ３２、Ｓ３３における場合とそれぞれ同様の処理が行われ、これにより、暗号処理手段１５０において得られた復号されたデジタルコンテンツは、バス１１０を介して、ＭＰＥＧコーデック１３０に供給される。

【００７２】ＭＰＥＧコーデック１３０では、ステップＳ４４において、デジタルコンテンツがＭＰＥＧデコード、すなわち伸長処理が実行され、入出力Ｉ／Ｆ１４０に供給される。入出力Ｉ／Ｆ１４０は、ステップＳ４４において、ＭＰＥＧコーデック１３０でＭＰＥＧデコードされたデジタルコンテンツを、内蔵するＡ／Ｄ，Ｄ／Ａコンバータ１４１でＤ／Ａ変換（Ｓ４５）して、アナログコンテンツとする。そして、ステップＳ４６に進み、入出力Ｉ／Ｆ１４０は、そのアナログコンテンツを、外部に出力し、再生処理を終了する。

【００７３】［トランスポートストリーム］次に、図５を用いて、トランスポートストリームデータを処理する場合における記録媒体上のデータフォーマットを説明する。記録媒体上のデータの読み書きの最小単位をブロック(block)という名前で呼ぶ。１ブロックは、１９２＊Ｘ（エックス）バイト（例えばＸ＝３２）の大きさとなっている。

【００７４】例えばＭＰＥＧ２のＴＳ（トランスポート・ストリーム）パケット（１８８バイト）にＡＴＳを付加して１９２バイトとして、それをＸ個集めて１ブロックのデータとする。ＡＴＳは２４乃至３２ビットの着信時刻を示すデータであり、Arrival Time Stamp（着信時刻スタンプ）の略である。ＡＴＳは各パケットの着信時刻に応じたランダム性のあるデータとして構成される。記録媒体のひとつのブロック（セクタ）には、ＡＴＳを付加したＴＳ（トランスポート・ストリーム）パケットをＸ個記録する。本発明の構成では、トランスポートストリームを構成する各ブロックの第１番目のＴＳパケットに付加されたＡＴＳを用いてそのブロック（セクタ）のデータを暗号化するブロックキーを生成する。

【００７５】ランダム性のあるＡＴＳを用いて暗号化用のブロックキーを生成することにより、ブロック毎に異なる固有キーが生成される。生成されたブロック固有キーを用いてブロック毎の暗号化処理を実行する。また、ＡＴＳを用いてブロックキーを生成する構成とすることにより、各ブロック毎の暗号化鍵を格納するための記録媒体上の領域が不要となり、メインデータ領域が有効に使用可能となる。さらに、データの記録、再生時にメインデータ部以外のデータをアクセスする必要もなくなり、処理が効率的になる。

【００７６】なお、図５に示すブロック・シード（Block Seed）は、ＡＴＳを含む付加情報である。ブロック・シードは、さらにＡＴＳだけでなく、図中段に示すようにコピー制限情報（ＣＣＩ：Copy Control Information）も付加する構成が可能である。この場合、ＡＴＳとＣＣＩを用いてブロックキーを生成する構成とすることができる。

【００７７】なお、本発明の構成においては、ＤＶＤ等の記録媒体上にデータを格納する場合、コンテンツの大部分のデータは暗号化されるが、図５の最下段に示すように、ブロックの先頭のｍ（たとえば、ｍ＝８または１６）バイトは暗号化されずに平文（Unencrypted data）のまま記録され、残りのデータ（ｍ＋１バイト以降）が暗号化される。これは暗号処理が８バイト単位としての処理であるために暗号処理データ長（Encrypted data）に制約が発生するためである。なお、もし、暗号処理が８バイト単位でなく、たとえば１バイト単位で行なえるなら、ｍ＝４として、ブロックシード以外の部分をすべて暗号化してもよい。

【００７８】［ＴＳ処理手段における処理］ここで、ＡＴＳの機能について詳細に説明する。ＡＴＳは、先にも説明したように入力トランスポートストリーム中の各トランスポートパケットの出現タイミングを保存するために付加する着信時刻スタンプである。

【００７９】すなわち、例えば複数のＴＶプログラム（コンテンツ）が多重化されたトランスポートストリー

ムの中から１つまたは幾つかのＴＶプログラム（コンテンツ）を取り出した時、その取り出したトランスポートストリームを構成するトランスポートパケットは、不規則な間隔で現れる（図７（ａ）参照）。トランスポートストリームは、各トランスポートパケットの出現タイミングに重要な意味があり、このタイミングはＭＰＥＧ２システムズ(ISO/IEC 13818-1)で規定されている仮想的なデコーダであるＴ－ＳＴＤ(Transport stream System Target Decoder)を破綻させないように符号化時に決定される。

【００８０】トランスポートストリームの再生時には、各トランスポートパケットに付加されたＡＴＳによって出現タイミングが制御される。従って、記録媒体にトランスポートパケットを記録する場合には、トランスポートパケットの入力タイミングを保存する必要があり、トランスポートパケットをＤＶＤ等の記録媒体に記録する時に、各トランスポートパケットの入力タイミングを表すＡＴＳを付加して記録する。

【００８１】図６に、デジタルインタフェース経由で入力されるトランスポートストリームをＤＶＤ等の記録媒体であるストレージメディアに記録する時のＴＳ処理手段３００において実行する処理を説明するブロック図を示す。端子６００からは、デジタル放送等のデジタルデータとしてトランスポートストリームが入力される。図１においては、入出力Ｉ／Ｆ１２０を介して、あるいは入出力Ｉ／Ｆ１４０、ＭＰＥＧコーデック１３０を介して端子６００からトランスポートストリームが入力される。

【００８２】トランスポートストリームは、ビットストリームパーサー(parser)６０２に入力される。ビットストリームパーサー６０２は、入力トランスポートストリームの中からＰＣＲ(Program Clock Reference)パケットを検出する。ここで、ＰＣＲパケットとは、ＭＰＥＧ２システムズで規定されているＰＣＲが符号化されているパケットである。ＰＣＲパケットは、１００ｍｓｅｃ以内の時間間隔で符号化されている。ＰＣＲは、トランスポートパケットが受信側に到着する時刻を２７ＭＨｚの精度で表す。

【００８３】そして、２７ＭＨｚＰＬＬ６０３において、記録再生器が持つ２７ＭＨｚクロックをトランスポートストリームのＰＣＲにロック（Lock）させる。タイムスタンプ発生回路６０４は、２７ＭＨｚクロックのクロックのカウント値に基づいたタイムスタンプを発生する。そして、ブロック・シード（Block seed）付加回路６０５は、トランスポートパケットの第1バイト目がスムージングバッファ６０６へ入力される時のタイムスタンプをＡＴＳとして、そのトランスポートパケットに付加する。

【００８４】ＡＴＳが付加されたトランスポートパケットは、スムージングバッファ６０６を通って、端子６０７から、暗号処理手段１５０に出力され、後段で説明する暗号処理が実行された後、記録媒体Ｉ／Ｆ２１０（図１）を介してストレージメディアである記録媒体２００に記録される。

【００８５】図7は、入力トランスポートストリームが記録媒体に記録される時の処理の例を示す。図７（ａ）は、ある特定プログラム（コンテンツ）を構成するトランスポートパケットの入力を示す。ここで横軸は、ストリーム上の時刻を示す時間軸である。この例ではトランスポートパケットの入力は、図７（ａ）に示すように不規則なタイミングで現れる。

【００８６】図７（ｂ）は、ブロック・シード（Block Seed）付加回路６０５の出力を示す。ブロック・シード（Block Seed）付加回路６０５は、トランスポートパケット毎に、そのパケットのストリーム上の時刻を示すＡＴＳを含むブロック・シード（Block Seed）を付加して、ソースパケットを出力する。図７（ｃ）は記録媒体に記録されたソースパケットを示す。ソースパケットは、図７（ｃ）に示すように間隔を詰めて記録媒体に記録される。このように間隔を詰めて記録することにより記録媒体の記録領域を有効に使用できる。

【００８７】図８は、記録媒体２００に記録されたトランスポートストリームを再生する場合のＴＳ処理手段３００の処理構成ブロック図を示している。端子８００からは、後段で説明する暗号処理手段において復号されたＡＴＳ付きのトランスポートパケットが、ブロック・シード（Block seed）分離回路８０１へ入力され、ＡＴＳとトランスポートパケットが分離される。タイミング発生回路８０４は、再生器が持つ２７ＭＨｚクロック８０５のクロックカウンター値に基づいた時間を計算する。

【００８８】なお、再生の開始時において、一番最初のＡＴＳが初期値として、タイミング発生回路８０４にセットされる。比較器８０３は、ＡＴＳとタイミング発生回路８０４から入力される現在の時刻を比較する。そして、タイミング発生回路８０４が発生する時間とＡＴＳが等しくなった時、出力制御回路８０２は、そのトランスポートパケットをＭＰＥＧコーデック１３０またはデジタル入出力Ｉ／Ｆ１２０へ出力する。

【００８９】図９は、入力ＡＶ信号を記録再生器１００のＭＰＥＧコーデック１３０においてＭＰＥＧエンコードして、さらにＴＳ処理手段３００においてトランスポートストリームを符号化する構成を示す。従って図９は、図１におけるＭＰＥＧコーデック１３０とＴＳ処理手段３００の両処理構成を併せて示すブロック図である。端子９０１からは、ビデオ信号が入力されており、それはＭＰＥＧビデオエンコーダ９０２へ入力される。

【００９０】ＭＰＥＧビデオエンコーダ９０２は、入力ビデオ信号をＭＰＥＧビデオストリームに符号化し、それをバッファビデオストリームバッファ９０３へ出力する。また、ＭＰＥＧビデオエンコーダ９０２は、ＭＰＥ

Ｇビデオストリームについてのアクセスユニット情報を多重化スケジューラ９０８へ出力する。ビデオストリームのアクセスユニットとは、ピクチャであり、アクセスユニット情報とは、各ピクチャのピクチャタイプ，符号化ビット量，デコードタイムスタンプである。ここで、ピクチャタイプは、Ｉ／Ｐ／Ｂピクチャ（picture）の情報である。また、デコードタイムスタンプは、ＭＰＥＧ２システムズで規定されている情報である。

【００９１】端子９０４からは、オーディオ信号が入力されており、それはＭＰＥＧオーディオエンコーダ９０５へ入力される。ＭＰＥＧオーディオエンコーダ９０５は、入力オーディオ信号をＭＰＥＧオーディオストリームに符号化し、それをバッファ９０６へ出力する。また、ＭＰＥＧオーディオエンコーダ９０５は、ＭＰＥＧオーディオストリームについてのアクセスユニット情報を多重化スケジューラ９０８へ出力する。オーディオストリームのアクセスユニットとは、オーディオフレームであり、アクセスユニット情報とは、各オーディオフレームの符号化ビット量，デコードタイムスタンプである。

【００９２】多重化スケジューラ９０８には、ビデオとオーディオのアクセスユニット情報が入力される。多重化スケジューラ９０８は、アクセスユニット情報に基づいて、ビデオストリームとオーディオストリームをトランスポートパケットに符号化する方法を制御する。多重化スケジューラ９０８は、内部に２７ＭＨｚ精度の基準時刻を発生するクロックを持ち、そして、ＭＰＥＧ２で規定されている仮想的なデコーダモデルであるＴ－ＳＴＤを満たすようにして、トランスポートパケットのパケット符号化制御情報を決定する。パケット符号化制御情報は、パケット化するストリームの種類とストリームの長さである。

【００９３】パケット符号化制御情報がビデオパケットの場合、スイッチ９７６はａ側になり、ビデオストリームバッファ９０３からパケット符号化制御情報により指示されたペイロードデータ長のビデオデータが読み出され、トランスポートパケット符号化器９０９へ入力される。

【００９４】パケット符号化制御情報がオーディオパケットの場合、スイッチ９７６はｂ側になり、オーディオストリームバッファ９０６から指示されたペイロードデータ長のオーディオデータが読み出され、トランスポートパケット符号化器９０９へ入力される。

【００９５】パケット符号化制御情報がＰＣＲパケットの場合、トランスポートパケット符号化器９０９は、多重化スケジューラ９０８から入力されるＰＣＲを取り込み、ＰＣＲパケットを出力する。パケット符号化制御情報がパケットを符号化しないことを指示する場合、トランスポートパケット符号化器９０９へは何も入力されない。

【００９６】トランスポートパケット符号化器９０９は、パケット符号化制御情報がパケットを符号化しないことを指示する場合、トランスポートパケットを出力しない。それ以外の場合、パケット符号化制御情報に基づいてトランスポートパケットを生成し、出力する。したがって、トランスポートパケット符号化器９０９は、間欠的にトランスポートパケットを出力する。到着（Arrival）タイムスタンプ（time stamp）計算手段９１０は、多重化スケジューラ９０８から入力されるＰＣＲに基づいて、トランスポートパケットの第1バイト目が受信側に到着する時刻を示すＡＴＳを計算する。

【００９７】多重化スケジューラ９０８から入力されるＰＣＲは、ＭＰＥＧ２で規定されるトランスポートパケットの１０バイト目の受信側への到着時刻を示すので、ＡＴＳの値は、ＰＣＲの時刻から１０バイト前のバイトが到着する時刻となる。

【００９８】ブロック・シード（Block Seed）付加回路９１１は、トランスポートパケット符号化器９０９から出力されるトランスポートパケットにＡＴＳを付加する。ブロック・シード（Block seed）付加回路９１１から出力されるＡＴＳ付きのトランスポートパケットは、スムージングバッファ９１２を通って、暗号処理手段１５０へ入力され、後段で説明する暗号処理が実行された後、ストレージメディアである記録媒体２００へ格納される。

【００９９】記録媒体２００へ格納されるＡＴＳ付きのトランスポートパケットは、暗号処理手段１５０で暗号化される前に図７（ｃ）に示すように間隔を詰めた状態で入力され、その後、記録媒体２００に格納される。トランスポートパケットが間隔を詰めて記録されても、ＡＴＳを参照することによって、そのトランスポートパケットの受信側への入力時刻を制御することができる。

【０１００】ところで、ＡＴＳの大きさは３２ビットに決まっているわけではなく、２４ビット乃至３１ビットでも構わない。ＡＴＳのビット長が長いほど、ＡＴＳの時間カウンターが一周する周期が長くなる。例えば、ＡＴＳが２７ＭＨｚ精度のバイナリーカウンターである場合、２４－ｂｉｔ長のＡＴＳが一周する時間は、約0.6秒である。この時間間隔は、一般のトランスポートストリームでは十分な大きさである。なぜなら、トランスポートストリームのパケット間隔は、ＭＰＥＧ２の規定により、最大０．１秒と決められているからである。しかしながら、十分な余裕を見て、ＡＴＳを２４－ｂｉｔ以上にしても良い。

【０１０１】このように、ＡＴＳのビット長を様々な長さとした場合、ブロックデータの付加データであるブロックシードの構成としていくつかの構成が可能となる。ブロック・シードの構成例を図１０に示す。図１０の例１は、ＡＴＳを３２ビット分使用する例である。図１０の例２は、ＡＴＳを３０ビットとし、コピー制御情報

（CCI）を２ビット分使用する例である。コピー制御情報は、それが付加されたデータのコピー制御の状態を表す情報であり、ＳＣＭＳ：Serial Copy Management SystemやＣＧＭＳ：Copy Generation Management Systemが有名である。これらのコピー制御情報では、その情報が付加されたデータは制限なくコピーが許可されていることを示すコピーフリー（Copy Free）、1世代のみのコピーを許可する1世代コピー許可（One Generation Copy Allowed）、コピーを認めないコピー禁止（Copy Prohibited）などの情報が表せる。

【０１０２】図１０に示す例３は、ＡＴＳを２４ビットとし、ＣＣＩを２ビット使用し、さらに他の情報を6ビット使用する例である。他の情報としては、たとえばこのデータがアナログ出力される際に、アナログ映像データのコピー制御機構であるマクロビジョン（Macrovision）のオン／オフ（On/Off）を示す情報など、様々な情報を利用することが可能である。

【０１０３】［キー配信構成としてのツリー（木）構造について］次に、図１に示した記録再生装置が、データを記録媒体に記録、もしくは記録媒体から再生する際に必要なキー、例えばメディアキーを、各機器に配布する構成について説明する。図１１は、本方式を用いた記録システムにおける記録再生装置の鍵の配布構成を示した図である。図１１の最下段に示すナンバ０～１５が個々の記録再生装置である。すなわち図１１に示す木（ツリー）構造の各葉（リーフ：leaf)がそれぞれの記録再生装置に相当する。

【０１０４】各デバイス０～１５は、製造時（出荷時）に、あらかじめ定められている初期ツリーにおける、自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノードキー）および各リーフのリーフキーを自身で格納する。図１１の最下段に示すＫ０００００～Ｋ１１１１が各デバイス０～１５にそれぞれ割り当てられたリーフキーであり、最上段のＫＲから、最下段から２番目の節（ノード）に記載されたキー：ＫＲ～Ｋ１１１をノードキーとする。

【０１０５】図１１に示すツリー構成において、例えばデバイス０はリーフキーＫ００００と、ノードキー：Ｋ０００、Ｋ００、Ｋ０、ＫＲを所有する。デバイス５はＫ０１０１、Ｋ０１０、Ｋ０１、Ｋ０、ＫＲを所有する。デバイス１５は、Ｋ１１１１、Ｋ１１１、Ｋ１１、Ｋ１、ＫＲを所有する。なお、図１１のツリーにはデバイスが０～１５の１６個のみ記載され、ツリー構造も４段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

【０１０６】また、図１１のツリー構造に含まれる各記録再生器には、様々な記録媒体、例えばＤＶＤ、ＣＤ、ＭＤ、メモリスティック（商標）等を使用する様々なタイプの記録再生器が含まれている。さらに、様々なアプリケーションサービスが共存することが想定される。このような異なるデバイス、異なるアプリケーションの共存構成の上に図１１に示すキー配布構成が適用されている。

【０１０７】これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図１１の点線で囲んだ部分、すなわちデバイス０，１，２，３を同一の記録媒体を用いるひとつのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、共通に使用するマスターキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、図１１の点線で囲んだ部分、すなわちデバイス０，１，２，３を１つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図１１のツリー中に複数存在する。

【０１０８】なお、ノードキー、リーフキーは、ある１つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

【０１０９】このツリー構造において、図１１から明らかなように、１つのグループに含まれる３つのデバイス０，１，２，３はノードキーとして共通のキーＫ００、Ｋ０、ＫＲを保有する。このノードキー共有構成を利用することにより、例えば共通のマスターキーをデバイス０，１，２，３のみに提供することが可能となる。たとえば、共通に保有するノードキーＫ００自体をマスターキーとして設定すれば、新たな鍵送付を実行することなくデバイス０，１，２，３のみが共通のマスターキーの設定が可能である。また、新たなマスターキーKmasterをノードキーＫ００で暗号化した値Ｅｎｃ（Ｋ００，Ｋmaster）を、ネットワークを介してあるいは記録媒体に格納してデバイス０，１，２，３に配布すれば、デバイス０，１，２，３のみが、それぞれのデバイスにおいて保有する共有ノードキーＫ００を用いて暗号Ｅｎｃ（Ｋ００，Kmaster）を解いてマスターキー：Kmasterを得ることが可能となる。なお、Ｅｎｃ（Ｋａ，Ｋｂ）はＫｂをＫａによって暗号化したデータであることを示す。

【０１１０】また、ある時点ｔにおいて、デバイス３の所有する鍵：Ｋ００１１，Ｋ００１，Ｋ００，Ｋ０，ＫＲが攻撃者（ハッカー）により解析されて露呈したことが発

覚した場合、それ以降、システム（デバイス０，１，２，３のグループ）で送受信されるデータを守るために、デバイス３をシステムから切り離す必要がある。そのためには、ノードキー：Ｋ００１，Ｋ００，Ｋ０，ＫＲをそれぞれ新たな鍵Ｋ（ｔ）００１，Ｋ（ｔ）００，Ｋ（ｔ）０，Ｋ（ｔ）Ｒに更新し、デバイス０，１，２にその更新キーを伝える必要がある。ここで、Ｋ（ｔ）ａａａは、鍵Ｋａａａの世代（Generation）：ｔの更新キーであることを示す。

【０１１１】更新キーの配布処理について説明する。キーの更新は、例えば、図１２（Ａ）に示す有効化キーブロック（ＥＫＢ：Enabling Key Block）と呼ばれるブロックデータによって構成されるテーブルをたとえばネットワーク、あるいは記録媒体に格納してデバイス０，１，２に供給することによって実行される。

【０１１２】図１２（Ａ）に示す有効化キーブロック（ＥＫＢ）には、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図１２の例は、図１１に示すツリー構造中のデバイス０，１，２において、世代ｔの更新ノードキーを配布することを目的として形成されたブロックデータである。図１１から明らかなように、デバイス０，デバイス１は、更新ノードキーとしてＫ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要であり、デバイス２は、更新ノードキーとしてＫ（ｔ）００１、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要である。

【０１１３】図１２（Ａ）のＥＫＢに示されるようにＥＫＢには複数の暗号化キーが含まれる。最下段の暗号化キーは、Ｅｎｃ（Ｋ００１０，Ｋ（ｔ）００１）である。これはデバイス２の持つリーフキーＫ００１０によって暗号化された更新ノードキーＫ（ｔ）００１であり、デバイス２は、自身の持つリーフキーによってこの暗号化キーを復号し、Ｋ（ｔ）００１を得ることができる。また、復号により得たＫ（ｔ）００１を用いて、図１２（Ａ）の下から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００１，Ｋ（ｔ）００）を復号可能となり、更新ノードキーＫ（ｔ）００を得ることができる。以下順次、図１２（Ａ）の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図１２（Ａ）の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号しＫ（ｔ）Ｒを得る。一方、デバイス０，１は、ノードキーＫ０００は更新する対象に含まれておらず、更新ノードキーとして必要なのは、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒである。デバイス０，１は、図１２（Ａ）の上から３段目の暗号化キーＥｎｃ（Ｋ０００，Ｋ（ｔ）００）を復号しＫ（ｔ）００、を取得し、以下、図１２（Ａ）の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図１２（Ａ）の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号しＫ（ｔ）Ｒを得る。このようにして、デバイス０，１，２は更新した鍵Ｋ（ｔ）Ｒを得ることができる。なお、図１２（Ａ）のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

【０１１４】図１１に示すツリー構造の上位段のノードキー：Ｋ（ｔ）０，Ｋ（ｔ）Ｒの更新が不要であり、ノードキーＫ００のみの更新処理が必要である場合には、図１２（Ｂ）の有効化キーブロック（ＥＫＢ：Enabling Key Block）を用いることで、更新ノードキーＫ（ｔ）００をデバイス０，１，２に配布することができる。

【０１１５】図１２（Ｂ）に示すＥＫＢは、例えば特定のグループにおいて共有する新たなマスターキー、あるいは記録媒体に固有のメディアキーを配布する場合に利用可能である。具体例として、図１１に点線で示すグループ内のデバイス０，１，２，３がある記録媒体を用いており、新たな共通のマスターキーＫ（ｔ）masterが必要であるとする。このとき、デバイス０，１，２，３の共通のノードキーＫ００を更新したＫ（ｔ）００を用いて新たな共通の更新マスターキー：Ｋ（ｔ）masterを暗号化したデータＥｎｃ（Ｋ（ｔ），Ｋ（ｔ）master）を図１２（Ｂ）に示すＥＫＢとともに配布する。この配布により、デバイス４など、その他のグループの機器においては復号されないデータとしての配布が可能となる。メディアキーについても同様である。

【０１１６】すなわち、デバイス０，１，２はＥＫＢを処理して得たＫ（ｔ）００を用いて上記暗号文を復号すれば、ｔ時点でのマスターキー：Ｋ（ｔ）masterやメディアキー：Ｋ（ｔ）mediaを得ることが可能になる。

【０１１７】［ＥＫＢを使用したメディアキーの取得］図１３に、本出願人の先の特許出願である特願平２０００－１０５３２８で提案したｔ時点でのメディアキーＫ（ｔ）mediaを得る処理例として、Ｋ（ｔ）００を用いて新たな共通のメディアキーＫ（ｔ）mediaを暗号化したデータＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）media）と図１２（Ｂ）に示すＥＫＢとを記録媒体を介して受領したデバイス２の処理を示す。

【０１１８】図１１に示すように、ある記録再生システムには、点線で囲まれた、デバイス０，１，２，３の４つの装置が含まれるとする。図１３は、デバイス３がリボークされたときに、記録媒体ごとに割り当てられるメディアキーを使用する場合に、記録再生装置（デバイス２）が記録媒体上のコンテンツを暗号化もしくは復号するために必要なメディアキーを、記録媒体に格納されているＥＫＢ（EnablingKey Block）と記録再生装置が記憶するデバイスキーを用いて求める際の処理を表している。

【０１１９】デバイス２のメモリには、自分にのみ割り当てられたリーフキーＫ_００１０と、それから木のルートまでの各ノード００１，００，０，Ｒのノードキー

（それぞれ、Ｋ_００１，Ｋ_００，Ｋ_０，Ｋ_Ｒ）が安全に格納されている。デバイス２は、図１３の記録媒体に格納されているＥＫＢのうち、インデックス（index）が００１０の暗号文を自分の持つリーフキーＫ_００１０で復号してノード００１のノードキーＫ（ｔ）_００１を計算し、次にそれを用いてインデックス（index）が００１の暗号文を復号してノード００のノードキーＫ（ｔ）_００を計算し、最後にそれを用いて暗号文を復号してメディアキーＫ（ｔ）_mediaを計算する必要がある。この計算回数は、リーフからメディアキーを暗号化するノードまでの深さが深くなるのに比例して増加する。すなわち、多くの記録再生装置が存在する大きなシステムにおいては多くの計算が必要となる。このようにして計算され、取得されたメディアキーを用いたデータの暗号化処理、復号処理態様について、以下、説明する。

【０１２０】［メディアキーを用いたコンテンツ記録処理］図１４の処理ブロック図に従って、暗号処理手段１５０が実行するデータの暗号化処理および記録媒体に対する記録処理の一例について説明する。

【０１２１】図１４に示す記録再生装置１００は自身の上述したＥＫＢに基づく算出処理によってメディアキーを取得する。

【０１２２】次に、記録再生装置１００は例えば光ディスクである記録媒体２００に識別情報としてのディスクＩＤ（Disc ID）が既に記録されているかどうかを検査する。記録されていれば、ディスクＩＤ（Disc ID）を読出し、記録されていなければ、暗号処理手段１５０においてランダムに、もしくはあらかじめ定められた例えば乱数発生等の方法でディスクＩＤ（Disc ID）を生成し、ディスクに記録する。ディスクＩＤ（Disc ID）はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。

【０１２３】記録再生器１００は、次にメディアキーとディスクＩＤを用いて、ディスク固有キー（Disc Unique Key）を生成する。ディスク固有キー（Disc Unique Key）の具体的な生成方法としては、図１５に示すように、ブロック暗号関数を用いたハッシュ関数にメディアキーとディスクＩＤ（Disc ID）を入力して得られた結果を用いる例１の方法や、FIPS 180-1で定められているハッシュ関数ＳＨＡ－１に、メディアキーとディスクＩＤ（Disc ID）とのビット連結により生成されるデータを入力し、その１６０ビットの出力から必要なデータ長のみをディスク固有キー（Disc Unique Key）として使用する例２の方法が適用できる。

【０１２４】次に、記録ごとの固有鍵であるタイトルキー（Title Key）を暗号処理手段１５０（図１参照）においてランダムに、もしくはあらかじめ定められた例えば乱数発生等の方法で生成し、ディスク２００に記録する。

【０１２５】次にディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）の組合せから、タイトル固有キー（Title Unique Key）を生成する。

【０１２６】このタイトル固有キー（Title Unique Key）生成の具体的な方法は、図１６に示すように、ブロック暗号関数を用いてディスク固有キーを鍵としてタイトルキーを暗号化して得られた結果を用いる例１の方法や、FIPS 180-1で定められているハッシュ関数ＳＨＡ－１に、メディアキーとディスクＩＤ（Disc ID）とのビット連結により生成されるデータを入力し、その１６０ビットの出力から必要なデータ長のみをタイトル固有キー（Title Unique Key）として使用する例２の方法が適用できる。

【０１２７】なお、上記の説明では、メディアキーとディスクＩＤ（Disc ID）からディスク固有キー（Disc Unique Key）を生成し、これとタイトルキー（Title Key）からタイトル固有キー（Title Unique Key）をそれぞれ生成するようにしているが、ディスク固有キー（Disc Unique Key）を不要としてメディアキーとディスクＩＤ（Disc ID）とタイトルキー（Title Key）から直接タイトル固有キー（Title Unique Key）を生成してもよく、また、タイトルキー（Title Key）を用いずに、メディアキー（Master Key）とディスクＩＤ（Disc ID）からタイトル固有キー（Title Unique Key）相当の鍵を生成してもよい。

【０１２８】さらに、図１４を用いて、その後の処理を説明する。被暗号化データとして入力されるブロックデータの先頭の第1～４バイトが分離されて出力されるブロックシード（Block Seed）と、先に生成したタイトル固有キー（Title Unique Key）とから、そのブロックのデータを暗号化する鍵であるブロック・キー（BlockKey）が生成される。

【０１２９】ブロック・キー（Block Key）の生成方法の例を図１７に示す。図１７では、いずれも３２ビットのブロック・シード（Block Seed）と、６４ビットのタイトル固有キー（Title Unique Key）とから、６４ビットのブロックキー（Block Key）を生成する例を２つ示している。

【０１３０】上段に示す例１は、鍵長６４ビット、入出力がそれぞれ６４ビットの暗号関数を使用している。タイトル固有キー（Title Unique Key）をこの暗号関数の鍵とし、ブロックシード（Block Seed）と３２ビットの定数（コンスタント）を連結した値を入力して暗号化した結果をブロックキー（Block Key）としている。

【０１３１】例２は、FIPS 180-1のハッシュ関数SHA-1を用いた例である。タイトル固有キー（Title Unique Key）とブロックシード（Block Seed）を連結した値をＳＨＡ－１に入力し、その１６０ビットの出力を、たとえば下位６４ビットのみ使用するなど、６４ビットに縮約したものをブロックキー（Block Key）としている。

【０１３２】なお、上記ではディスク固有キー（Disc Unique key）、タイトル固有キー（Title Unique Key）、ブロックキー（Block Key）をそれぞれ生成する例を説明したが、たとえば、ディスク固有キー（Disc Unique Key）とタイトル固有キー（Title Unique Key）の生成を実行することなく、ブロックごとにメディアキーとディスクＩＤ（Disc ID）とタイトルキー（Title Key）とブロックシード（Block Seed）を用いてブロックキー（Block Key）を生成してもよい。

【０１３３】ブロックキーが生成されると、生成されたブロックキー（Block Key）を用いてブロックデータを暗号化する。図１４の下段に示すように、ブロックシード（Block Seed）を含むブロックデータの先頭の第1～mバイト（たとえばm＝８バイト）は分離（セレクタ１６０８）されて暗号化対象とせず、m＋１バイト目から最終データまでを暗号化する。なお、暗号化されないmバイト中にはブッロク・シードとしての第1～４バイトも含まれる。セレクタにより分離された第m＋１バイト以降のブロックデータは、暗号処理手段１５０に予め設定された暗号化アルゴリズムに従って暗号化される。暗号化アルゴリズムとしては、たとえばFIPS 46-2で規定されるＤＥＳ（Data Encryption Standard）を用いることができる。

【０１３４】以上の処理により、コンテンツはブロック単位で、世代管理されたメディアキー、ブロック・シード等に基づいて生成されるブロックキーで暗号化が施されて記録媒体に格納される。

【０１３５】次に、記録した暗号化コンテンツデータに対して、記録再生装置は自身に割り当てられた公開鍵暗号系の秘密鍵（署名生成鍵）を用いてデジタル署名を計算し、これを自身の公開鍵証明書およびコンテンツデータと共に記録媒体に記録する。デジタル署名の生成方法としては、たとえば、IEEE P1363 で規格制定中のＥＣ－ＤＳＡ(Elliptic Curve Digital Signature Algorithm) を用いることができる。図１８にコンテンツの記録処理の概要を説明するフローチャートを示す。

【０１３６】まず、記録再生装置はステップＳ１０１において記録対象コンテンツの暗号化処理を実行する。コンテンツ暗号化は、図１４を用いて説明したように、ブロックキーを用いたブロックデータの暗号化処理として実行される。

【０１３７】さらに、ステップＳ１０２において、記録再生装置は自身に割り当てられた公開鍵暗号系の秘密鍵（署名生成鍵）を用いて暗号化コンテンツに対するデジタル署名を計算する。デジタル署名の生成方法としては、たとえば、IEEE P1363 で規格制定中のＥＣ－ＤＳＡ(Elliptic Curve Digital Signature Algorithm)が適用可能である。

【０１３８】次に、ステップＳ１０３において、記録再生装置は生成したデジタル署名と公開鍵証明書を記録コンテンツに対応付けて記録媒体に記録し、ステップＳ１０４において暗号化データの記録媒体に対する記録処理（Ｓ１０２）を実行する。

【０１３９】さらに、図１９に暗号化コンテンツにデジタル署名を実行して記録を実行する場合の詳細処理フローを示す。

【０１４０】ステップＳ２０１において、記録再生装置は前述のＥＫＢ処理（図１３参照）によってメディアキーを取得する。

【０１４１】Ｓ２０２において、記録媒体に識別情報としてのディスクＩＤ（Disc ID）が既に記録されているかどうかを検査する。記録されていればＳ２０３でこのディスクＩＤを読出し、記録されていなければＳ２０４で、ランダムに、もしくはあらかじめ定められた方法でディスクＩＤを生成し、ディスクに記録する。次に、Ｓ２０５では、メディアキーとディスクＩＤを用いて、ディスク固有キーを生成する。ディスク固有キーは先に説明したように、例えば、FIPS 180-1で定められているハッシュ関数ＳＨＡ－１を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法（図１５参照）などを適用することで求める。

【０１４２】次にＳ２０６に進み、その一回の記録ごとの固有の鍵としてのタイトルキー（Title Key）を生成し、生成したタイトルキーをディスク（記録媒体）に記録する。次にＳ２０７で、上記のディスク固有キーとタイトルキーとから、タイトル固有キーを生成（図１６参照）する。

【０１４３】Ｓ２０８では、記録再生装置は記録すべきコンテンツデータの被暗号化データをＴＳパケットの形で受信する。Ｓ２０９で、ＴＳ処理手段３００は、各ＴＳパケットを受信した時刻情報であるＡＴＳを付加する。あるいはコピー制御情報ＣＣＩとＡＴＳ、さらに他の情報を組み合わせた値を付加する。次に、Ｓ２１０で、ＡＴＳを付加したＴＳパケットを順次受信し、１ブロックを形成する例えばＸ＝３２に達したか、あるいはパケットの終了を示す識別データを受信したかを判定する。いずれかの条件が満足された場合はステップＳ２１１に進み、Ｘ個、あるいはパケット終了までのパケットを並べて、１ブロックのブロックデータを形成する。

【０１４４】次に、暗号処理手段１５０は、Ｓ２１２で、ブロックデータの先頭の３２ビット（ＡＴＳを含むブロック・シード）とＳ２０７で生成したタイトル固有キーとから、そのブロックのデータを暗号化する鍵であるブロックキーを生成（図１７参照）する。

【０１４５】Ｓ２１３では、ブロックキーを用いてＳ２１１で形成したブロックデータを暗号化する。なお、先にも説明したように、暗号化の対象となるのは、ブロックデータのm＋１バイト目から最終データまでである。暗号化アルゴリズムは、たとえばFIPS 46-2で規定されるＤＥＳ（Data Encryption Standard）が適用される。

【０１４６】Ｓ２１４で、記録ブロックが第1ブロックであるか否かを判定し、第1ブロックである場合は、Ｓ２１５においてブロックデータをデジタル署名対象データとして、デジタル署名を生成し、公開鍵証明書とともに記録媒体に記録する。デジタル署名の生成処理は例えばIEEE P1363で規格制定中のＥＣ－ＤＳＡ(Elliptic Curve Digital Signature Algorithm)を適用する。

【０１４７】Ｓ２１６で、暗号化したブロックデータを記録媒体に記録する。Ｓ２１７で、全データを記録したかを判断する。全データを記録していれば、記録処理を終了し、全データを記録していなければＳ２０８に戻って残りのデータの処理を実行する。

【０１４８】以上の処理により、コンテンツが暗号化されて記録媒体に記録され、さらに、暗号化コンテンツのブロックデータに対するデジタル署名、および公開鍵証明書が記録媒体に記録されることになる。

【０１４９】なお、記録媒体に格納されるコンテンツ、タイトルキー、デジタシル署名、公開鍵証明書、その他コンテンツ関連データはそれぞれの対応が識別可能な構成をもって記録される。例えば管理データをテーブルとして記録媒体に記録することによって対応付けが可能である。図２０に記録コンテンツに関する対応データのアドレスデータをテーブルとして記録する場合のテーブル構成例を示す。

【０１５０】図２０に示すように、各コンテンツはコンテンツ関連データとともに、ファイルとして管理され、コンテンツデータのアドレス、タイトルキーのアドレス、デジタル署名のアドレス、公開鍵証明書のアドレス、その他ファイル情報について記録されたテーブルが生成され記録媒体に格納される。

【０１５１】次に、記録媒体に暗号化コンテンツを記録する際に、暗号化コンテンツに署名を実行するのではなく、コンテンツに対応して生成されるタイトルキーにデジタル署名を実行してコンテンツ記録を実行する処理について、図２１のフローを用いて説明する。

【０１５２】ステップＳ３０１において、記録再生装置は前述のＥＫＢ処理（図１３参照）によってメディアキーを取得する。

【０１５３】Ｓ３０２において、記録媒体に識別情報としてのディスクＩＤ（Disc ID）が既に記録されているかどうかを検査する。記録されていればＳ３０３でこのディスクＩＤを読出し、記録されていなければＳ３０４で、ランダムに、もしくはあらかじめ定められた方法でディスクＩＤを生成し、ディスクに記録する。次に、Ｓ３０５では、メディアキーとディスクＩＤを用いて、ディスク固有キーを生成する。ディスク固有キーは先に説明したように、例えば、FIPS 180-1で定められているハッシュ関数ＳＨＡ－１を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法（図１５参照）などを適用することで求める。

【０１５４】次にＳ３０６に進み、その一回の記録ごとの固有の鍵としてのタイトルキー（Title Key）を生成し、生成したタイトルキーに対するデジタル署名を実行する。デジタル署名の生成処理は例えばIEEE P1363で規格制定中のＥＣ－ＤＳＡ(Elliptic Curve Digital Signature Algorithm)を適用する。さらに、生成したタイトルキー、デジタル署名、および公開鍵証明書を記録媒体（ディスク）に格納する。

【０１５５】次にＳ３０７で、上記のディスク固有キーとタイトルキーとから、タイトル固有キーを生成（図１６参照）する。

【０１５６】Ｓ３０８では、記録再生装置は記録すべきコンテンツデータの被暗号化データをＴＳパケットの形で受信する。Ｓ３０９で、ＴＳ処理手段３００は、各ＴＳパケットを受信した時刻情報であるＡＴＳを付加する。あるいはコピー制御情報ＣＣＩとＡＴＳ、さらに他の情報を組み合わせた値を付加する。次に、Ｓ３１０で、ＡＴＳを付加したＴＳパケットを順次受信し、１ブロックを形成する例えばＸ＝３２に達したか、あるいはパケットの終了を示す識別データを受信したかを判定する。いずれかの条件が満足された場合はステップＳ３１１に進み、Ｘ個、あるいはパケット終了までのパケットを並べて、１ブロックのブロックデータを形成する。

【０１５７】次に、暗号処理手段１５０は、Ｓ３１２で、ブロックデータの先頭の３２ビット（ＡＴＳを含むブロック・シード）とＳ３０７で生成したタイトル固有キーとから、そのブロックのデータを暗号化する鍵であるブロックキーを生成（図１７参照）する。

【０１５８】Ｓ３１３では、ブロックキーを用いてＳ３１１で形成したブロックデータを暗号化する。なお、先にも説明したように、暗号化の対象となるのは、ブロックデータのｍ＋１バイト目から最終データまでである。暗号化アルゴリズムは、たとえばFIPS 46-2で規定されるＤＥＳ（Data Encryption Standard）が適用される。

【０１５９】Ｓ３１４で、暗号化したブロックデータを記録媒体に記録する。Ｓ３１５で、全データを記録したかを判断する。全データを記録していれば、記録処理を終了し、全データを記録していなければＳ３０８に戻って残りのデータの処理を実行する。

【０１６０】以上の処理により、コンテンツが暗号化されて記録媒体に記録され、さらに、暗号化コンテンツに対応するタイトルキーに対するデジタル署名、および公開鍵証明書が記録媒体に記録されることになる。

【０１６１】上記の例ではタイトルキーにデジタル署名を施したが、タイトルキーとディスクＩＤに対してデジタル署名を施してもよい。このようにすることにより、そのデータがそのディスクに記録されたということを明確にでき、そのデータが他のディスクにコピーされたものは不正なコピーであるという判断が容易に行える。

【０１６２】［メディアキーを用いたコンテンツ再生処

理］次に、記録媒体に格納された暗号化コンテンツデータの復号および再生処理を図２２以下を用いて説明する。

【０１６３】再生処理においては、再生装置はまず、再生するコンテンツデータと共に記録されている記録装置の公開鍵証明書とデジタル署名を読出し、これらの正当性を確認する。

【０１６４】すなわち、再生装置が保持している、信頼できるセンタの公開鍵（署名検証鍵）を用いて公開鍵証明書の正当性を検査し、これに成功すれば、公開鍵証明書に含まれている、記録装置の公開鍵（署名検証鍵）を用いて記録装置が作成して記録したデジタル署名を検査する。デジタル署名の検査方法としては、たとえば、前述のＥＣ－ＤＳＡを用いることができる。

【０１６５】次に、再生装置は、記録されている公開鍵証明書から記録装置の識別情報（ＩＤ）を読出し、これとリボケーション情報からこの記録装置がシステムからリボーク（排除）されていないことを確認する。

【０１６６】（リボケーションリストを用いたリボーク検査）リボケーション情報としては、たとえば図２３に示すリボケーションリストを用いることができる。リボケーションリストは図に示すようにリボーク（排除）する機器のＩＤを併記したデータと、リストのバージョンナンバーに対してセンタがデジタル署名を施したものである。このリボケーションリストは、たとえば、１）製造される機器（記録再生装置）のメモリに記憶させる。さらに、２）ニンテンツデータと一緒にネットワークや記録媒体を介して流通させる。などの方法で、システム内を流通させることにより、再生処理時に再生装置がより新しいリボケーション情報を得られるようにしておく。

【０１６７】また、リボケーションリストを使用する際には、リストが偽造、改ざんされたものでないことを検査するために、リボケーションリスト内に格納されたセンタの署名の検証処理を実行する。署名の検証処理は、公開鍵証明書の署名検証と同様、予め機器（記録再生装置）が持っているセンタの公開鍵（署名検証鍵）を用いて検査することが可能である。

【０１６８】（ＥＫＢを利用したリボーク検査）また、リボケーション情報を図２３に示すようなリストとして各機器に配布する構成をとらず、リボークされているか否かをＥＫＢを使用して判別する構成としてもよい。たとえば図１１に示したツリー状に機器が配置されたシステムにおいて、図１２の（Ａ）例１に示すＥＫＢが記録媒体に格納されていたとする。このとき、各機器は、ＥＫＢのインデックスを逐次みていくと、ＥＫＢで更新されるノードキーをツリー状に表したものが図２４の太線のようになることが理解できる。

【０１６９】そして、更新されたノードキーを得られるのは、太線で示したツリーのリーフ（葉）の下に位置する機器だけ、つまり、デバイス０，１，２だけであることが理解できる。そして、それ以外の機器はシステムからリボークされていると判断することができ、これらのＩＤを持った機器が記録したコンテンツデータの再生を禁止する処理を、再生処理の実行時に実行することによりリボーク機器による記録コンテンツの再配布を停止することが可能となる。なお、この例では、図１１におけるリーフの位置と、デバイスのＩＤが対応していることを前提としている。すなわち、有効化キーブロック（ＥＫＢ）のインデックスのトレース処理を前記ＩＤに基づいて実行することでリボークの有無を判別する。

【０１７０】トレース処理によるリボーク検査について詳細に説明する。まず、図２５に有効化キーブロック（ＥＫＢ）のフォーマット例を示す。バージョン１００１は、有効化キーブロック（ＥＫＢ）のバージョンを示す識別子である。なお、バージョンは最新のＥＫＢを識別する機能とコンテンツとの対応関係を示す機能を持つ。デプス１００２は、有効化キーブロック（ＥＫＢ）の配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ１００３は、有効化キーブロック（ＥＫＢ）中のデータ部の位置を示すポインタであり、タグポインタ１００４はタグ部の位置、署名ポインタ１００５は署名の位置を示すポインタである。

【０１７１】データ部１００６は、例えば更新するノードキーを暗号化したデータを格納する。例えば図１３に示すような更新されたノードキーに関する各暗号化キー等を格納する。

【０１７２】タグ部１００７は、データ部に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図２６を用いて説明する。図２６では、データとして先に図１２（Ａ）で説明した有効化キーブロック（ＥＫＢ）を送付する例を示している。この時のデータは、図２６の表（ｂ）に示すようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルートキーの更新キーＫ（ｔ）Ｒが含まれているので、トップノードアドレスはＫＲとなる。このとき、例えば最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）は、図２６の（ａ）に示す階層ツリーに示す位置にある。ここで、次のデータは、Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが０、ない場合は１が設定される。タグは｛左（Ｌ）タグ，右（Ｒ）タグ｝として設定される。最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）の左にはデータがあるので、Ｌタグ＝０、右にはデータがないので、Ｒタグ＝１となる。以下、すべてのデータにタグが設定され、図２６（ｃ）に示すデータ列、およびタグ列が構成される。

【０１７３】タグは、データＥｎｃ（Ｋｘｘｘ，Ｋｙｙｙ）がツリー構造のどこに位置しているのかを示すため

に設定されるキー配置識別タグである。データ部に格納されるキーデータＥｎｃ（Ｋｘｘｘ，Ｋｙｙｙ）．．．は、単純に暗号化されたキーの羅列データに過ぎないので、上述したタグによってデータとして格納された暗号化キーのツリー上の位置を判別可能としたものである。上述したタグを用いずに、先の図１２で説明した構成のように暗号化データに対応させたノード・インデックスを用いて、例えば、

０：Ｅｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）ｒｏｏｔ）

００：Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）

０００：Ｅｎｃ（Ｋ（（ｔ）０００，Ｋ（Ｔ）００）

．．．のようなデータ構成とすることも可能であるが、このようなインデックスを用いた構成とすると冗長なデータとなりデータ量が増大し、ネットワークを介する配信等においては好ましくない。これに対し、上述したタグをキー位置を示す索引データとして用いることにより、少ないデータ量でキー位置の判別が可能となる。

【０１７４】図２５に戻って、ＥＫＢフォーマットについてさらに説明する。署名（Signature）は、有効化キーブロック（ＥＫＢ）を発行したＥＫＢ発行局、例えば認証局、鍵管理センタ、コンテンツロバイダ、決済機関等が実行する電子署名である。ＥＫＢを受領したデバイスは署名検証によって正当な有効化キーブロック（ＥＫＢ）発行者が発行した有効化キーブロック（ＥＫＢ）であることを確認する。

【０１７５】図２６に関する説明から理解されるようにＥＫＢ内に格納されたタグは自ノードの左及び右のノードの鍵データの有無を０，１で示している。すなわちデータがある場合は０、データがない場合を１として設定される。リーフＩＤに基づくＥＫＢの追跡処理、すなわち辿り方は、このような条件設定に基づくタグを用いて行われる。

【０１７６】リーフＩＤに基づくＥＫＢの追跡（辿り方）について、図２７を用いて説明する。図２７（ａ）に示すようにリーフキーＫ１００１を持つデバイスをリボークデバイス［１００１］とする。このとき、ＥＫＢは、図２７（ｂ）のような暗号化キーとタグの構成を持つ。図２７（ｂ）のＥＫＢは、図２７（ａ）の１つのデバイス［１００１］をリボークするために、ＫＲ，Ｋ１，Ｋ１０，Ｋ１００を更新したＥＫＢとなる。

【０１７７】このＥＫＢを処理することにより、リボークデバイス［１００１］以外のリーフはすべて更新されたルートキーＫ（ｔ）Ｒを取得できる。すなわち、ノードキーＫ０の下位につらなるリーフは、更新されていないノードキーＫ０をデバイス内に保持しているので、Ｅｎｃ（Ｋ０，Ｋ（ｔ）Ｒ）をＫ０によって復号することで更新ルートキーＫ（ｔ）Ｒを取得可能となる。また、Ｋ１１以下のリーフは更新されていないＫ１１を用いて、Ｅｎｃ（Ｋ１１，Ｋ（ｔ）１）をＫ１１によって復号することで更新ノードキーＫ（ｔ）１を取得して、さらに、Ｅｎｃ（Ｋ（ｔ）１，Ｋ（ｔ）Ｒ）をＫ（ｔ）１によって復号することで更新ルートキーを取得できる。Ｋ１０１の下位リーフについても復号ステップが１つ増加するのみで、同様に更新ルートキーを取得できる。

【０１７８】また、リボークされていないリーフキーＫ１０００を持つデバイス［１０００］は、自己のリーフキーで、Ｅｎｃ（Ｋ１０００，Ｋ（ｔ）１００）を復号して、Ｋ（ｔ）１００を取得後、上位のノードキーを順次復号して更新ルートキーを取得できる。

【０１７９】リボークされたデバイス［１００１］のみが、自己のリーフの一段上の更新ノードキーＫ（ｔ）１００をＥＫＢ処理により取得できないので、結局、更新ルートキーＫ（ｔ）Ｒを取得することができない。

【０１８０】リボークされていない正当なデバイスには、図２７（ｂ）に示すデータ部と、タグを有するＥＫＢがＥＫＢ発行局から配信され、デバイス内に格納されている。

【０１８１】リボーク検証を行なおうとするデバイスは、図２７（ａ）のリボークデバイス［ＩＤ＝１００１］の公開鍵証明書の検証の後、公開鍵証明書からＩＤを取得する。このＩＤは［１００１］であり、ＥＫＢ配信ツリー構成のリーフ位置を示している。

【０１８２】ＩＤ［１００１］を取り出したデバイスは、ＩＤ＝１００１のリーフに対応するデバイスが、ＥＫＢにおいて有効なリーフデバイスとして設定されているかを検証する。この検証は、すなわち、リーフ［１００１］が更新されたルートキーＫ（ｔ）Ｒを取得できるか否かを判定する処理として実行される。

【０１８３】例えば、非更新ノードキー（ｅｘ．図２７（ａ）のＫ０，Ｋ１１など）の下位に属するリーフであれば、リボークされていないことが明らかであり、正当デバイスであると判定可能であり、更新ノードキーの下位に属するリーフである場合は、その更新ノードキーを取得可能な暗号化データがＥＫＢに格納されているか否かによって、そのエンティティがリボークされているか否かを判定可能となる。

【０１８４】判定処理の一例として、ＥＫＢに格納されたタグに基づいてＥＫＢ追跡処理を行なう例を説明する。ＥＫＢ追跡処理は、上位のルートキーからキー配信ツリーを辿れるか否かを判定する処理である。例えば図２７のリーフ［１００１］のＩＤである［１００１］を［1］、［0］、［0］、［1］の４ビットとして、最上位ビットから順次下位ビットに従ってツリーを辿る。ビットが１であれば右側、０であれば左に進む。

【０１８５】図２７（ａ）のルートから、ＩＤ［１００１］の最上位ビットは１であり、右側に進む。ＥＫＢ内の最初のタグは、０：｛0，0｝であり、両枝にデータを有することが判定され、右側に進みＫ１に辿り着ける。次にＫ１の下位のノードに進む。ＩＤ［１００１］の２番目のビットは０であり、左側に進む。Ｋ１の下位

のデータ有無を示すタグは、図２７（ａ），（ｂ）の２：｛０，０｝であり、両枝にデータを有すると判定され、左側に進みＫ１０に辿り着ける。さらに、ＩＤ［１００１］の３番目のビットは０であり、左側に進む。Ｋ１０の下位のデータ有無を示すタグは、図２７（ａ），（ｂ）の３：｛０，０｝であり、両枝にデータを有すると判定され、左側に進みＫ１００に辿り着ける。さらに、ＩＤ［１００１］の最下位ビットは１であり、右側に進む。Ｋ１００の下位のデータ有無を示すタグは、図２７（ａ），（ｂ）の５：｛０，１｝であり、右側にはデータを持たない。従ってノード［１００１］には辿りつけないことが判定され、ＩＤ［１００１］のデバイスはＥＫＢによる更新ルートキーを取得できないデバイス、すなわちリボークデバイスであると判定される。

【０１８６】例えば図２７（ａ）のリーフキーＫ１０００を有するデバイスＩＤは［１０００］であり、上述と同様のＥＫＢ内のタグに基づくＥＫＢ追跡処理、すなわちツリーを辿る処理を実行すると、ノード［１０００］に辿りつくことができるので、ＥＫＢによる更新ルートキーを取得可能なリボークされていない正当なデバイスであると判定される。

【０１８７】また、例えば更新されていないノードキー、例えばＫ０，Ｋ１１などの下位のリーフにも、リーフ自体には、辿り着けないが、この場合は、更新されていない末端ノードに辿りつくことが可能である。更新されていないノードの下位のリーフは、更新されていないノードキーを用いてＥＫＢの処理が可能であり、更新ルートキーを取得できるので正当なデバイスである。更新されていないノードキーであるか否かは、そのノードに対応するタグにより判定することが可能となる。更新されていないノードキーＫ０，Ｋ１１，Ｋ１０１に対応するタグは１：｛１，１｝、４：｛１，１｝、６｛１，１｝となり、これらはさらに下位ノードまたはリーフが存在するが、ＥＫＢ内には暗号化鍵データを持たないことを示しており、これらの下位のリーフのデバイスはリボークされていない有効な正当デバイスであると判定される。

【０１８８】図２７に示す例は、１つのデバイスについてのみのリボーク態様であるが、図２８に示すようにあるノードの下にあるすべてのリーフデバイスを一括してリボークすることも可能である。この場合のＥＫＢのデータ（暗号化キー）、タグは図２８（ｂ）のようになる。

【０１８９】例えば、デバイスがリボークされたＫ１０００に対応するリーフデバイスの公開鍵証明書からＩＤ［１０００］を取得したとすると、このＩＤ［１０００］に基づいてＥＫＢのタグに基づいてツリーを辿る処理を実行する。

【０１９０】図２８（ａ）のルートから、ＩＤ［１０００］の最上位ビットは１であり、右側に進む。ＥＫＢ内の最初のタグ０：｛０，０｝であり、両枝にデータを有することが判定され、右側に進みＫ１に辿り着ける。次にＫ１の下位のノードに進む。ＩＤ［１０００］の２番目のビットは０であり、左側に進む。Ｋ１の下位のデータ有無を示すタグは、図１３（ａ），（ｂ）の２：｛１，０｝であり、左側にはデータを持たない。従ってノード［１０００］には辿りつけない。このときの末端ノードＫ１に対応するタグは｛１，０｝であり、下位のデータを持たない｛１，１｝ではない。

【０１９１】タグ｛１，０｝は、Ｋ１の右側の下位のノードまたはリーフにおいてのみ復号可能な更新されたＫ１（ｔ）を取得するための暗号化鍵データがＥＫＢに格納されていることを示している。

【０１９２】このように、リーフＩＤに基づいて辿り着く最終地点がノードであり、その最終ノードの対応タグが｛１，１｝以外の値を持っている場合は、さらに下位の暗号化鍵データをＥＫＢ内に有することを示している。この場合は、そのＩＤを持つリーフデバイスはＥＫＢの処理によって更新されたルートキーを取得することができないので、リボークされたデバイスであると判定される。

【０１９３】このようにして、認証処理において通信相手から取得した公開鍵証明書に格納されたリーフＩＤに基づいて通信相手がリボークされているか否かを判定することが可能となる。

【０１９４】図２９にＥＫＢを利用したリボークデバイス判定処理についての処理フローを示す。フローの各ステップについて説明する。ステップＳ３５１において、検査対象の公開鍵証明書からＩＤを取得する。ステップＳ３５２において、取得したＩＤを用いＥＫＢのタグに基づいて、ＩＤの示すリーフまたはリードを目標とする追跡処理を実行する。

【０１９５】追跡処理は、前述の図２７，図２８を用いて説明した手順で実行する。追跡処理の結果、ＩＤの示すリーフまたはノードに辿り着くことができたか、辿りつけない場合であってもＩＤの示すリーフまたはノードにおいてＥＫＢ処理が可能であるか否か、すなわち更新ルートキーの取得が可能か否かを判定する（Ｓ３５３）。

【０１９６】ＥＫＢ処理が可能である位置にあるＩＤであると判定されれば、ステップＳ３５４に進み、ＩＤに対応するデバイスはリボークされていない正当なデバイスであると判定する。一方、ＥＫＢ処理が不可能な位置にあるＩＤであると判定されれば、ステップＳ３５５に進み、ＩＤに対応するデバイスはリボークされている不正なデバイスであると判定する。

【０１９７】なお、上述の追跡処理では、ＥＫＢのタグ部は利用しているがデータ部は利用していない。これを用いて、リボケーション情報を表す目的では、図２５に示す通常のＥＫＢではなく、データ部のないＥＫＢを用

いることにより、それ用のＥＫＢのサイズを小さくできる。もちろん、図２５に示す、通常の、コンテンツを保護するためのＥＫＢをリボケーション情報を表すために用いることも可能である。

【０１９８】上述したように、リボーケーションリスト、あるいはＥＫＢツリーのトレース処理に従ったリボーク検査により記録媒体に対してコンテンツの記録を行なった機器がリボークされているかいないかの検証を行なう。コンテンツの記録を行なった機器がリボークされてないことが検証されたことを条件として再生装置はコンテンツデータの再生処理を継続する。再生処理においては、図１４を用いて説明した暗号化および記録処理と同様、メディアキーとディスクＩＤからディスク固有キーを生成し、ディスク固有キーと、タイトルキーからタイトル固有キーを生成し、さらにタイトルキーと記録媒体から読み取られるブロックシードとから、ブロックキーを生成して、ブロックキーを復号キーとして用い、記録媒体２００から読み取られるブロック単位の暗号化データの復号処理を実行する。

【０１９９】再生処理の概要について図３０のフローチャートを用いて説明する。まず、ステップＳ４０１において再生装置は、再生対象コンテンツを記録した記録媒体に格納されたコンテンツ記録装置の公開鍵証明書およびデジタル署名の検証を実行する。検証は、まず、公開鍵証明書のセンタ署名をセンタの公開鍵を用いて実行し、公開鍵証明書の正当性が確認された後、公開鍵証明書中に格納されたコンテンツ記録装置の公開鍵を取り出して、コンテンツ記録者のデジタル署名の検証を実行する。いずれの検証もＯＫであれば次ステップに進み、いずれかの検証がＮＧであれば、以降のステップ実行が禁止され再生処理はストップする。

【０２００】次に、ステップＳ４０２においてコンテンツ記録装置のリボケーション検査を実行する。このリボケーション検査は、例えば予め再生装置に格納された図２３に示したリボケーションリストに格納された機器ＩＤと、公開鍵証明書内の機器ＩＤに一致するものがあるか否かを検査することによって行われる。あるいは、前述のＥＫＢツリー構成によるツリー探索処理を実行してもよい。ステップＳ４０２のリボケーション検査においてコンテンツ記録装置がリボークされていないと判定されると次ステップに進み、リボークされている場合は、以降のステップ実行が禁止され再生処理はストップする。

【０２０１】ステップＳ４０２のリボケーション検査においてコンテンツ記録装置がリボークされていないと判定された場合、ステップＳ４０３において暗号化コンテンツの記録媒体からの読み出しが実行され、ステップＳ４０４において暗号化コンテンツの復号処理が実行されてコンテンツの再生が行われる。

【０２０２】このように、記録媒体に格納されたコンテンツ再生処理に際し、コンテンツ記録装置のリボーク状況を判定してリボークされていない機器によって記録されたコンテンツの再生のみを実行する構成としたので、不正に記録されたコンテンツが無秩序に流通利用されることが防止される。また、リボーク判定は、公開鍵証明書に格納されたＩＤによって判定され、その信頼性は維持される。

【０２０３】次に、図３１を用いて暗号化コンテンツに対してデジタル署名が実行された記録コンテンツの再生を実行する場合の詳細処理について説明する。

【０２０４】ステップＳ５０１において、再生装置は記録媒体からメディアキー、ディスクＩＤを読み出し、ステップＳ５０２において、タイトルキー、デジタル署名、公開鍵証明書の読み出しを実行する。署名、公開鍵証明書が存在しない場合（Ｓ５０３：Ｎｏ）は、正当な記録処理によるコンテンツではないと判定され、以降の処理の実行が停止され再生処理は終了する。

【０２０５】署名、公開鍵証明書が存在した場合（Ｓ５０３：Ｙｅｓ）は、ステップＳ５０４において公開鍵証明書の検証が実行される。公開鍵証明書の検証は、再生装置が保有する公開鍵証明書の発行管理を行なうセンタ（認証局）の公開鍵を用いて実行される。公開鍵証明書の検証がＯＫであり正当性が確認されると次ステップに進む。正当性検証がＮＧの場合は、以降の処理の実行が停止され再生処理は終了する。

【０２０６】次に、ステップＳ５０５では、公開鍵証明書からコンテンツ記録を実行した記録装置の識別子（ＩＤ）が取り出され、リボーク検査を行なう。リボーク検査は前述の図２３のリボークリストあるいはツリー探索処理のいずれかによって実行される。コンテンツの記録装置のリボークがないと判定されると次ステップに進み、リボークありと判定されると、以降の処理の実行が停止され再生処理は終了する。

【０２０７】次に、Ｓ５０６では、メディアキーとディスクＩＤを用いて、ディスク固有キーを生成する。ディスク固有キーは先に説明したように、例えば、FIPS 180-1で定められているハッシュ関数ＳＨＡ－１を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法（図１５参照）などを適用することで求める。

【０２０８】次にＳ５０７に進みタイトルキー（Title Key）を読み出し、読み出したタイトルキーとディスク固有キーから、タイトル固有キーを生成（図１６参照）する。

【０２０９】Ｓ５０８では、再生装置は再生すべきコンテンツデータのブロックデータを読み出す。Ｓ５０９で読み出しブロックが第1ブロックであるか否かを判定し、第1ブロックである場合には、ステップＳ５１０において第1ブロックに対して生成されたコンテンツ記録者（記録装置）のデジタル署名の検証を実行する。デジタル署名の検証は、正当性の検証された公開鍵証明書か

ら取り出したコンテンツ記録装置の公開鍵を用いて実行される。デジタル署名の検証がＯＫであり正当性が確認されると次ステップに進む。正当性検証がＮＧの場合は、以降の処理の実行が停止され再生処理は終了する。

【０２１０】ステップＳ５１１では、ブロックデータの先頭の３２ビット（ＡＴＳを含むブロック・シード）とＳ５０７で生成したタイトル固有キーとから、そのブロックのデータを復号する鍵であるブロックキーを生成（図１７参照）する。

【０２１１】Ｓ５１２では、ブロックキーを用いてブロックデータを復号する。復号アルゴリズムは、たとえばFIPS 46-2で規定されるＤＥＳ（Data Encryption Standard）が適用される。

【０２１２】Ｓ５１３で、全データを読み出したかを判断する。全データを読み出していれば、再生処理を終了し、全データを読み出していなければＳ５０８に戻って残りのデータの処理を実行する。

【０２１３】このように、公開鍵証明書の検証、コンテンツ記録装置のリボークの判定、暗号化コンテンツのブロックデータに対するデジタル署名の検証が順次実行され、すべての条件が満足したことに基づいてコンテンツの正当性が判定され、暗号化コンテンツの記録媒体からの復号、再生処理が実行されることになる。

【０２１４】次に、図３２を用いてタイトルキーに対してデジタル署名が実行された記録コンテンツの再生を実行する場合の詳細処理について説明する。

【０２１５】ステップＳ６０１において、再生装置は記録媒体からメディアキー、ディスクＩＤを読み出し、ステップＳ６０２において、タイトルキー、デジタル署名、公開鍵証明書の読み出しを実行する。署名、公開鍵証明書が存在しない場合（Ｓ６０３：Ｎｏ）は、正当な記録処理によるコンテンツではないと判定され、以降の処理の実行が停止され再生処理は終了する。

【０２１６】署名、公開鍵証明書が存在した場合（Ｓ６０３：Ｙｅｓ）は、ステップＳ６０４において公開鍵証明書の検証が実行される。公開鍵証明書の検証は、再生装置が保有する公開鍵証明書の発行管理を行なうセンタ（認証局）の公開鍵を用いて実行される。公開鍵証明書の検証がＯＫであり正当性が確認されると次ステップに進む。正当性検証がＮＧの場合は、以降の処理の実行が停止され再生処理は終了する。

【０２１７】次に、ステップＳ６０５では、公開鍵証明書からコンテンツ記録を実行した記録装置の識別子（ＩＤ）が取り出され、リボーク検査を行なう。リボーク検査は前述の図２３のリボークリストあるいはツリー探索処理のいずれかによって実行される。コンテンツの記録装置のリボークがないと判定されると次ステップに進み、リボークありと判定されると、以降の処理の実行が停止され再生処理は終了する。

【０２１８】次に、ステップＳ６０６においてタイトルキーに対して実行されたコンテンツ記録者（記録装置）のデジタル署名の検証を実行する。デジタル署名の検証は、正当性の検証された公開鍵証明書から取り出したコンテンツ記録装置の公開鍵を用いて実行される。デジタル署名の検証がＯＫであり正当性が確認されると次ステップに進む。正当性検証がＮＧの場合は、以降の処理の実行が停止され再生処理は終了する。

【０２１９】次に、Ｓ６０７では、メディアキーとディスクＩＤを用いて、ディスク固有キーを生成する。ディスク固有キーは先に説明したように、例えば、FIPS 180-1で定められているハッシュ関数ＳＨＡ－１を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法（図１５参照）などを適用することで求める。

【０２２０】次にＳ６０８に進みタイトルキー（Title Key）を読み出し、読み出したタイトルキーとディスク固有キーから、タイトル固有キーを生成（図１６参照）する。

【０２２１】Ｓ６０９では、再生装置は再生すべきコンテンツデータのブロックデータを読み出す。ステップＳ６１０では、ブロックデータの先頭の３２ビット（ＡＴＳを含むブロック・シード）とＳ６０８で生成したタイトル固有キーとから、そのブロックのデータを復号する鍵であるブロックキーを生成（図１７参照）する。

【０２２２】Ｓ６１１では、ブロックキーを用いてブロックデータを復号する。復号アルゴリズムは、たとえばFIPS 46-2で規定されるＤＥＳ（Data Encryption Standard）が適用される。

【０２２３】Ｓ６１２で、全データを読み出したかを判断する。全データを読み出していれば、再生処理を終了し、全データを読み出していなければＳ６０９に戻って残りのデータの処理を実行する。

【０２２４】このように、公開鍵証明書の検証、コンテンツ記録装置のリボークの判定、暗号化コンテンツのタイトルキーに対するデジタル署名の検証が順次実行され、すべての条件が満足したことに基づいてコンテンツの正当性が判定され、暗号化コンテンツの記録媒体からの復号、再生処理が実行されることになる。

【０２２５】上述のように、コンテンツデータの記録媒体に対する記録時の暗号化処理、および記録媒体からの再生時の復号処理においては、ＥＫＢに基づいてメディアキーを算出し、その後算出したメディアキーと他の識別子等に基づいて、コンテンツの暗号化処理用の鍵、または復号処理用の鍵を生成する。

【０２２６】なお、上述した例では、メディアキーを用いてコンテンツデータの暗号化処理、および復号処理に用いるキーを生成する構成を説明したが、メディアキーではなく、複数の記録再生装置に共通のマスターキー、あるいは記録再生器固有のデバイスキーをＥＫＢから取得して、これらに基づいてコンテンツデータの暗号化処理、および復号処理に用いるキーを生成する構成として

もよい。さらに、ＥＫＢから取得されるメディアキー、マスターキー、あるいはデバイスキー自体をコンテンツデータの暗号化処理、および復号処理に用いるキーとして適用することも可能である。

【０２２７】上述のように、本発明においては、記録再生装置がデータを情報記録媒体に記録する際に自身のデジタル署名および公開鍵証明書をデータと共に記録するようにした。このことにより、情報を記録する際には、必ず、どの記録装置が記録したかという証拠もデータと共に記録するようにしているので、もし不正に記録されたデータを含む記録媒体が流通したとしても、それをどの記録装置が記録したか特定できるので、システムからの排除が行える。

【０２２８】さらに、記録再生装置がデータを読み出す際に上記デジタル署名および公開鍵証明書の正当性を確認し、さらに記録装置がシステムからリボークされていないことを確認した後にデータを読み出す構成とした。このことにより、不正な記録装置が、不正な記録データに対してデジタル署名を記録しないような攻撃を無力なものにしているとともに、不正な装置で記録されたデータを正当な装置で再生しないようにすることで、不正な装置のシステムからの排除をより強力に行っている。

【０２２９】［記録処理におけるコピー制御］さて、コンテンツの著作権者等の利益を保護するには、ライセンスを受けた装置において、コンテンツのコピーを制御する必要がある。

【０２３０】即ち、コンテンツを記録媒体に記録する場合には、そのコンテンツが、コピーしても良いもの（コピー可能）かどうかを調査し、コピーして良いコンテンツだけを記録するようにする必要がある。また、記録媒体に記録されたコンテンツを再生して出力する場合には、その出力するコンテンツが、後で、違法コピーされないようにする必要がある。

【０２３１】そこで、そのようなコンテンツのコピー制御を行いながら、コンテンツの記録再生を行う場合の図１の記録再生装置の処理について、図３３および図３４のフローチャートを参照して説明する。

【０２３２】まず、外部からのディジタル信号のコンテンツを、記録媒体に記録する場合においては、図３３（Ａ）のフローチャートにしたがった記録処理が行われる。図３３（Ａ）の処理について説明する。図１の記録再生器１００を例として説明する。ディジタル信号のコンテンツ（ディジタルコンテンツ）が、例えば、IEEE1394シリアルバス等を介して、入出力Ｉ／Ｆ１２０に供給されると、ステップＳ７０１において、入出力Ｉ／Ｆ１２０は、そのディジタルコンテンツを受信し、ステップＳ７０２に進む。

【０２３３】ステップＳ７０２では、入出力Ｉ／Ｆ１２０は、受信したディジタルコンテンツが、コピー可能であるかどうかを判定する。即ち、例えば、入出力Ｉ／Ｆ１２０が受信したコンテンツが暗号化されていない場合（例えば、上述のＤＴＣＰを使用せずに、平文のコンテンツが、入出力Ｉ／Ｆ１２０に供給された場合）には、そのコンテンツは、コピー可能であると判定される。

【０２３４】また、記録再生装置１００がＤＴＣＰに準拠している装置であるとし、ＤＴＣＰに従って処理を実行するものとする。ＤＴＣＰでは、コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ（Encryption Mode Indicator）が規定されている。ＥＭＩが００Ｂ（Ｂは、その前の値が２進数であることを表す）である場合は、コンテンツがコピーフリーのもの（Copy-freely）であることを表し、ＥＭＩが０１Ｂである場合には、コンテンツが、それ以上のコピーをすることができないもの（No-more-copies）であることを表す。さらに、ＥＭＩが１０Ｂである場合は、コンテンツが、１度だけコピーして良いもの（Copy-one-generation）であることを表し、ＥＭＩが１１Ｂである場合には、コンテンツが、コピーが禁止されているもの（Copy-never）であることを表す。

【０２３５】記録再生装置１００の入出力Ｉ／Ｆ１２０に供給される信号にＥＭＩが含まれ、そのＥＭＩが、Copy-freelyやCopy-one-generationであるときには、コンテンツはコピー可能であると判定される。また、ＥＭＩが、No-more-copiesやCopy-neverであるときには、コンテンツはコピー可能でないと判定される。

【０２３６】ステップＳ７０２において、コンテンツがコピー可能でないと判定された場合、ステップＳ７０３～Ｓ７０５をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体１０に記録されない。

【０２３７】また、ステップＳ７０２において、コンテンツがコピー可能であると判定された場合、ステップＳ７０３に進み、以下、ステップＳ７０３～Ｓ７０５において、図３（Ａ）のステップＳ１２、Ｓ１３、Ｓ１４における処理と同様の処理が行われる。すなわち、ＴＳ処理手段３００によるトランスポートパケットに対するＡＴＳ付加、暗号処理手段１５０における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体１９５に記録して、記録処理を終了する。

【０２３８】なお、ＥＭＩは、入出力Ｉ／Ｆ１２０に供給されるディジタル信号に含まれるものであり、ディジタルコンテンツが記録される場合には、そのディジタルコンテンツとともに、ＥＭＩ、あるいは、ＥＭＩと同様にコピー制御状態を表す情報（例えば、ＤＴＣＰにおけるembedded CCIなど）も記録される。

【０２３９】この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。

【０２４０】本発明の記録再生装置では、このＥＭＩやembedded CCIなどのコピー制御情報を、ＴＳパケットに

付加する形で記録する。即ち、図１０の例２や例３のように、ＡＴＳを２４ビットないし３０ビット分と、コピー制御情報を加えた３２ビットを図５に示すように各ＴＳパケットに付加する。

【０２４１】外部からのアナログ信号のコンテンツを、記録媒体に記録する場合においては、図３３（Ｂ）のフローチャートにしたがった記録処理が行われる。図３３（Ｂ）の処理について説明する。アナログ信号のコンテンツ（アナログコンテンツ）が、入出力Ｉ／Ｆ１４０に供給されると、入出力Ｉ／Ｆ１４０は、ステップＳ７１１において、そのアナログコンテンツを受信し、ステップＳ７１２に進み、受信したアナログコンテンツが、コピー可能であるかどうかを判定する。

【０２４２】ここで、ステップＳ７１２の判定処理は、例えば、入出力Ｉ／Ｆ１４０で受信した信号に、マクロビジョン(Macrovision)信号や、ＣＧＭＳ－Ａ(Copy Generation Management System-Analog)信号が含まれるかどうかに基づいて行われる。即ち、マクロビジョン信号は、ＶＨＳ方式のビデオカセットテープに記録すると、ノイズとなるような信号であり、これが、入出力Ｉ／Ｆ１４０で受信した信号に含まれる場合には、アナログコンテンツは、コピー可能でないと判定される。

【０２４３】また、例えば、ＣＧＭＳ－Ａ信号は、ディジタル信号のコピー制御に用いられるＣＧＭＳ信号を、アナログ信号のコピー制御に適用した信号で、コンテンツがコピーフリーのもの(Copy-freely)、１度だけコピーして良いもの(Copy-one-generation)、またはコピーが禁止されているもの(Copy-never)のうちのいずれであるかを表す。

【０２４４】従って、ＣＧＭＳ－Ａ信号が、入出力Ｉ／Ｆ１４０で受信した信号に含まれ、かつ、そのＣＧＭＳ－Ａ信号が、Copy-freelyやCopy-one-generationを表している場合には、アナログコンテンツは、コピー可能であると判定される。また、ＣＧＭＳ－Ａ信号が、Copy-neverを表している場合には、アナログコンテンツは、コピー可能でないと判定される。

【０２４５】さらに、例えば、マクロビジョン信号も、ＣＧＭＳ－Ａ信号も、入出力Ｉ／Ｆ４で受信した信号に含まれない場合には、アナログコンテンツは、コピー可能であると判定される。

【０２４６】ステップＳ７１２において、アナログコンテンツがコピー可能でないと判定された場合、ステップＳ７１３乃至Ｓ７１７をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体１０に記録されない。

【０２４７】また、ステップＳ７１２において、アナログコンテンツがコピー可能であると判定された場合、ステップＳ７１３に進み、以下、ステップＳ７１３乃至Ｓ７１７において、図３（Ｂ）のステップＳ２２乃至Ｓ２６における処理と同様の処理が行われ、これにより、コンテンツがデジタル変換、ＭＰＥＧ符号化、ＴＳ処理、暗号化処理がなされて記録媒体に記録され、記録処理を終了する。

【０２４８】なお、入出力Ｉ／Ｆ１４０で受信したアナログ信号に、ＣＧＭＳ－Ａ信号が含まれている場合に、アナログコンテンツを記録媒体に記録するときには、そのＣＧＭＳ－Ａ信号も、記録媒体に記録される。即ち、図１０で示したＣＣＩもしくはその他の情報の部分に、この信号が記録される。この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。ただし、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

【０２４９】［再生処理におけるコピー制御］次に、記録媒体に記録されたコンテンツを再生して、ディジタルコンテンツとして外部に出力する場合においては、図３４（Ａ）のフローチャートにしたがった再生処理が行われる。図３４（Ａ）の処理について説明する。まず最初に、ステップＳ８０１、Ｓ８０２、Ｓ８０３において、図４（Ａ）のステップＳ３１、Ｓ３２、Ｓ３３における処理と同様の処理が行われ、これにより、記録媒体から読み出された暗号化コンテンツが暗号処理手段１５０において復号処理がなされ、ＴＳ処理がなされる。各処理が実行されたディジタルコンテンツは、バス１１０を介して、入出力Ｉ／Ｆ１２０に供給される。

【０２５０】入出力Ｉ／Ｆ１２０は、ステップＳ８０４において、そこに供給されるディジタルコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、入出力Ｉ／Ｆ１２０に供給されるディジタルコンテンツにＥＭＩ、あるいは、ＥＭＩと同様にコピー制御状態を表す情報（コピー制御情報）が含まれない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

【０２５１】また、例えば、入出力Ｉ／Ｆ１２０に供給されるディジタルコンテンツにＥＭＩが含まれる場合、従って、コンテンツの記録時に、ＤＴＣＰの規格にしたがって、ＥＭＩが記録された場合には、そのＥＭＩ（記録されたＥＭＩ(Recorded EMI)）が、Copy-freelyであるときには、ディジタルコンテンツは、後でコピー可能なものであると判定される。また、ＥＭＩが、No-more-copiesであるときには、コンテンツは、後でコピー可能なものでないと判定される。

【０２５２】なお、一般的には、記録されたＥＭＩが、Copy-one-generationやCopy-neverであることはない。Copy-one-generationのＥＭＩは記録時にNo-more-copiesに変換され、また、Copy-neverのＥＭＩを持つディジタルコンテンツは、記録媒体に記録されないからである。ただし、システムにおいてたとえば「Copy-one-generat

ionのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

【０２５３】ステップＳ８０４において、コンテンツが、後でコピー可能なものであると判定された場合、ステップＳ８０５に進み、入出力Ｉ／Ｆ１２０は、そのディジタルコンテンツを、外部に出力し、再生処理を終了する。

【０２５４】また、ステップＳ８０４において、コンテンツが、後でコピー可能なものでないと判定された場合、ステップＳ８０６に進み、入出力Ｉ／Ｆ１２０は、例えば、ＤＴＣＰの規格等にしたがって、ディジタルコンテンツを、そのディジタルコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

【０２５５】即ち、例えば、上述のように、記録されたＥＭＩが、No-more-copiesである場合（もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたＥＭＩがCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

【０２５６】このため、入出力Ｉ／Ｆ１２０は、ＤＴＣＰの規格にしたがい、相手の装置との間で認証を相互に行い、相手が正当な装置である場合（ここでは、ＤＴＣＰの規格に準拠した装置である場合）には、ディジタルコンテンツを暗号化して、外部に出力する。

【０２５７】次に、記録媒体に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図３４（Ｂ）のフローチャートにしたがった再生処理が行われる。図３４（Ｂ）の処理について説明する。ステップＳ８１１乃至Ｓ８１５において、図４（Ｂ）のステップＳ４１乃至Ｓ４５における処理と同様の処理が行われる。すなわち、暗号化コンテンツの読み出し、復号処理、ＴＳ処理、ＭＰＥＧデコード、Ｄ／Ａ変換が実行される。これにより得られるアナログコンテンツは、入出力Ｉ／Ｆ１４０で受信される。

【０２５８】入出力Ｉ／Ｆ１４０は、ステップＳ８１６において、そこに供給されるコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、記録されていたコンテンツにＥＭＩなどのコピー制御情報がいっしょに記録されていない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

【０２５９】また、コンテンツの記録時に、例えばＤＴＣＰの規格にしたがって、ＥＭＩまたはコピー制御情報が記録された場合には、その情報が、Copy-freelyであるときには、コンテンツは、後でコピー可能なものであると判定される。

【０２６０】また、ＥＭＩまたはコピー制御情報が、No-more-copiesである場合、もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたＥＭＩまたはコピー制御情報がCopy-one-generationである場合には、コンテンツは、後でコピー可能なものでないと判定される。

【０２６１】さらに、例えば、入出力Ｉ／Ｆ１４０に供給されるアナログコンテンツにＣＧＭＳ－Ａ信号が含まれる場合、従って、コンテンツの記録時に、そのコンテンツとともにＣＧＭＳ－Ａ信号が記録された場合には、そのＣＧＭＳ－Ａ信号が、Copy-freelyであるときには、アナログコンテンツは、後でコピー可能なものであると判定される。また、ＣＧＭＳ－Ａ信号が、Copy-neverであるときには、アナログコンテンツは、後でコピー可能なものでないと判定される。

【０２６２】ステップＳ８１６において、コンテンツが、後でコピー可能であると判定された場合、ステップＳ８１７に進み、入出力Ｉ／Ｆ１４０は、そこに供給されたアナログ信号を、そのまま外部に出力し、再生処理を終了する。

【０２６３】また、ステップＳ８１６において、コンテンツが、後でコピー可能でないと判定された場合、ステップＳ８１８に進み、入出力Ｉ／Ｆ１４０は、アナログコンテンツを、そのアナログコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

【０２６４】即ち、例えば、上述のように、記録されたＥＭＩ等のコピー制御情報が、No-more-copiesである場合（もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたＥＭＩ等のコピー制御情報がCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

【０２６５】このため、入出力Ｉ／Ｆ１４０は、アナログコンテンツを、それに、例えば、マクロビジョン信号や、Copy-neverを表すＧＣＭＳ－Ａ信号を付加して、外部に出力する。また、例えば、記録されたＣＧＭＳ－Ａ信号が、Copy-neverである場合にも、コンテンツは、それ以上のコピーは許されない。このため、入出力Ｉ／Ｆ１４０は、ＣＧＭＳ－Ａ信号をCopy-neverに変更して、アナログコンテンツとともに、外部に出力する。

【０２６６】以上のように、コンテンツのコピー制御を行いながら、コンテンツの記録再生を行うことにより、コンテンツに許された範囲外のコピー（違法コピー）が行われることを防止することが可能となる。

【０２６７】［データ処理手段の構成］なお、上述した一連の処理は、ハードウェアにより行うことは勿論、ソフトウェアにより行うこともできる。即ち、例えば、暗号処理手段１５０は暗号化／復号ＬＳＩとして構成する

ことも可能であるが、汎用のコンピュータや、１チップのマイクロコンピュータにプログラムを実行させることにより行う構成とすることも可能である。同様にＴＳ処理手段３００も処理をソフトウェアによって実行することが可能である。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータや１チップのマイクロコンピュータ等にインストールされる。図３５は、上述した一連の処理を実行するプログラムがインストールされるコンピュータの一実施の形態の構成例を示している。

【０２６８】プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク２００５やＲＯＭ２００３に予め記録しておくことができる。あるいは、プログラムはフロッピー（登録商標）ディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体２０１０に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体２０１０は、いわゆるパッケージソフトウエアとして提供することができる。

【０２６９】なお、プログラムは、上述したようなリムーバブル記録媒体２０１０からコンピュータにインストールする他、ダウンロードサイトから、ディジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、ＬＡＮ(Local AreaNetwork)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部２００８で受信し、内蔵するハードディスク２００５にインストールすることができる。

【０２７０】コンピュータは、ＣＰＵ(Central Processing Unit)２００２を内蔵している。ＣＰＵ２００２には、バス２００１を介して、入出力インタフェース２０１１が接続されており、ＣＰＵ２００２は、入出力インタフェース２０１０を介して、ユーザによって、キーボードやマウス等で構成される入力部２００７が操作されることにより指令が入力されると、それにしたがって、ＲＯＭ(Read Only Memory)２００３に格納されているプログラムを実行する。

【０２７１】あるいは、ＣＰＵ２００２は、ハードディスク２００５に格納されているプログラム、衛星若しくはネットワークから転送され、通信部２００８で受信されてハードディスク２００５にインストールされたプログラム、またはドライブ２００９に装着されたリムーバブル記録媒体２０１０から読み出されてハードディスク２００５にインストールされたプログラムを、ＲＡＭ(Random Access Memory)２００４にロードして実行する。

【０２７２】これにより、ＣＰＵ２００２は、上述したフローチャートにしたがった処理、あるいは上述したブロック図の構成により行われる処理を行う。そして、ＣＰＵ２００２は、その処理結果を、必要に応じて、例えば、入出力インタフェース２０１１を介して、ＬＣＤ(Liquid CryStal Display)やスピーカ等で構成される出力部２００６から出力、あるいは、通信部２００８から送信、さらには、ハードディスク２００５に記録させる。

【０２７３】ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。

【０２７４】また、プログラムは、１のコンピュータにより処理されるものであっても良いし、複数のコンピュータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

【０２７５】なお、本実施の形態では、コンテンツの暗号化／復号を行うブロックを、１チップの暗号化／復号ＬＳＩで構成する例を中心として説明したが、コンテンツの暗号化／復号を行うブロックは、例えば、図１に示すＣＰＵ１７０が実行する１つのソフトウェアモジュールとして実現することも可能である。同様に、ＴＳ処理手段３００の処理もＣＰＵ１７０が実行する１つのソフトウェアモジュールとして実現することが可能である。

【０２７６】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０２７７】

【発明の効果】以上、説明したように、本発明の構成によれば情報記録装置がデータを情報記録媒体に記録する際に自身のデジタル署名および公開鍵証明書をデータと共に記録する。このことにより、情報を記録する際には、必ず、どの記録装置が記録したかという証拠もデータと共に記録するようにした。情報再生装置は、コンテンツの復号処理以前に署名および公開鍵証明書の正当性を確認し、コンテンツ記録者を特定し、公開鍵証明書、デジタル署名の改竄の無いことを確認する。本構成により、不正な記録装置による記録コンテンツの利用（再生）の効率的排除が可能となる。また、不正に記録されたデータを含む記録媒体が流通したとしても、それをどの記録装置が記録したか特定できるので、システムからの排除が行える。

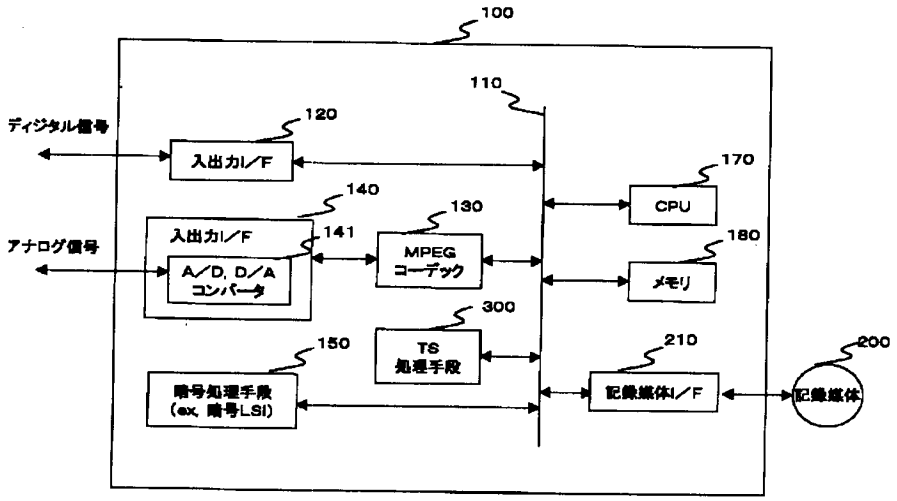
【図面の簡単な説明】

【図１】本発明の情報記録再生装置の構成例を示すブロック図である。

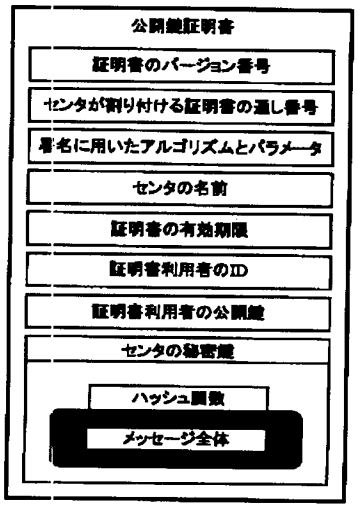
【図２】本発明の情報記録再生装置において適用される公開鍵証明書の例を示す図である。
【図３】本発明の情報記録再生装置のデータ記録処理フローを示す図である。
【図４】本発明の情報記録再生装置のデータ再生処理フローを示す図である。
【図５】本発明の情報記録再生装置において処理されるデータフォーマットを説明する図である。
【図６】本発明の情報記録再生装置におけるトランスポート・ストリーム（ＴＳ）処理手段の構成を示すブロック図である。
【図７】本発明の情報記録再生装置において処理されるトランスポート・ストリームの構成を説明する図である。
【図８】本発明の情報記録再生装置におけるトランスポート・ストリーム（ＴＳ）処理手段の構成を示すブロック図である。
【図９】本発明の情報記録再生装置におけるトランスポート・ストリーム（ＴＳ）処理手段の構成を示すブロック図である。
【図１０】本発明の情報記録再生装置において処理されるブロックデータの付加情報としてのブロック・データの構成例を示す図である。
【図１１】本発明の情報記録再生装置に対するＥＫＢ配信処理について説明するツリー構成図である。
【図１２】本発明の情報記録再生装置に対するキー配布に使用されるＥＫＢの例を示す図である。
【図１３】本発明の情報記録再生装置におけるメディアキーのＥＫＢを使用した配布例と復号処理例を示す図である。
【図１４】本発明の情報記録再生装置におけるメディアキーを使用したデータ記録処理時の暗号化処理を説明するブロック図である。
【図１５】本発明の情報記録再生装置において適用可能なディスク固有キーの生成例を説明する図である。
【図１６】本発明の情報記録再生装置において、適用可能なタイトル固有キーの生成処理例を示す図である。
【図１７】本発明の情報記録再生装置において適用可能なブロック・キーの生成方法を説明する図である。
【図１８】本発明の情報記録再生装置におけるデータ記録処理時の暗号化処理を説明するブロック図である。
【図１９】本発明の情報記録再生装置において暗号化コンテンツに対する署名を生成してデータ記録を行なう処理を説明するフロー図である。
【図２０】本発明の情報記録再生装置において記録される暗号化コンテンツと公開鍵証明書、署名等との対応を管理するテーブルの構成例を示す図である。
【図２１】本発明の情報記録再生装置においてタイトルキーに対する署名を生成してデータ記録を行なう処理を説明するフロー図である。
【図２２】本発明の情報記録再生装置におけるデータ再生処理時の復号処理を説明するブロック図である。
【図２３】本発明の情報記録再生装置において利用されるリボケーションテーブルの構成例を示す図である。
【図２４】本発明の情報記録再生装置においてＥＫＢ配信ツリーをリボークデバイスの検査に適用さする場合の処理を説明する図である。
【図２５】本発明の情報記録再生装置において適用可能な有効化キーブロック（ＥＫＢ）のフォーマット例を示す図である。
【図２６】有効化キーブロック（ＥＫＢ）のタグの構成を説明する図である。
【図２７】リボークエンティテイ判定のためのＥＫＢ追跡処理について説明する図（例１）である。
【図２８】リボークエンティテイ判定のためのＥＫＢ追跡処理について説明する図（例２）である。
【図２９】リボークエンティテイ判定のためのＥＫＢ追跡処理について説明するフロー図である。
【図３０】本発明の情報記録再生装置において署名を検証してデータ再生を行なう処理を説明するフロー図である。
【図３１】本発明の情報記録再生装置において暗号化コンテンツに対する署名を検証してデータ再生を行なう処理を説明するフロー図である。
【図３２】本発明の情報記録再生装置においてタイトルキーに対する署名を検証してデータ再生を行なう処理を説明するフロー図である。
【図３３】本発明の情報記録再生装置におけるデータ記録処理時のコピー制御処理を説明するフローチャートである。
【図３４】本発明の情報記録再生装置におけるデータ再生処理時のコピー制御処理を説明するフローチャートである。
【図３５】本発明の情報記録再生装置において、データ処理をソフトウェアによって実行する場合の処理手段構成を示したブロック図である。
【符号の説明】
１００　記録再生装置
１１０　バス
１２０　入出力Ｉ／Ｆ
１３０　ＭＰＥＧコーデック
１４０　入出力Ｉ／Ｆ
１４１　Ａ／Ｄ，Ｄ／Ａコンバータ
１５０　暗号処理手段
１６０　ＲＯＭ
１７０　ＣＰＵ
１８０　メモリ
１９０　ドライブ
２００　記録媒体
２１０　記録媒体Ｉ／Ｆ

３００　ＴＳ処理手段
６００，６０７　端子
６０２　ビットストリームパーサー
６０３　ＰＬＬ
６０４　タイムスタンプ発生回路
６０５　ブロックシード付加回路
６０６　スムージングバッファ
８００，８０６　端子
８０１　ブロックシード分離回路
８０２　出力制御回路
８０３　比較器
８０４　タイミング発生回路
８０５　２７ＭＨｚクロック
９０１，９０４，９１３　端子
９０２　ＭＰＥＧビデオエンコーダ
９０３　ビデオストリームバッファ
９０５　ＭＰＥＧオーディオエンコーダ
９０６　オーディオストリームバッファ
９０８　多重化スケジューラ
９０９　トランスポートパケット符号化器
９１０　到着タイムスタンプ計算手段
９１１　ブロックシード付加回路
９１２　スムージングバッファ
９７６　スイッチ
１００１　バージョン
１００２　デプス
１００３　データポインタ
１００４　タグポインタ
１００５　署名ポインタ
１００６　データ部
１００７　タグ部
１００８　署名
２００１　バス
２００２　ＣＰＵ
２００３　ＲＯＭ
２００４　ＲＡＭ
２００５　ハードディスク
２００６　出力部
２００７　入力部
２００８　通信部
２００９　ドライブ
２０１０　リムーバブル記録媒体
２０１１　入出力インタフェース

【図１】

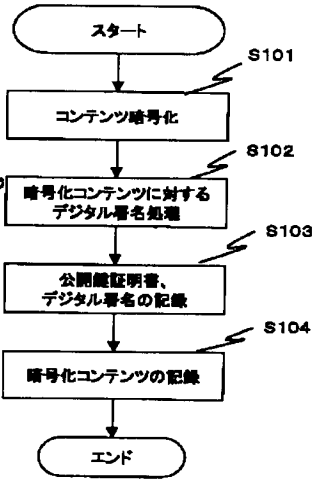


【図２】




公開鍵証明書

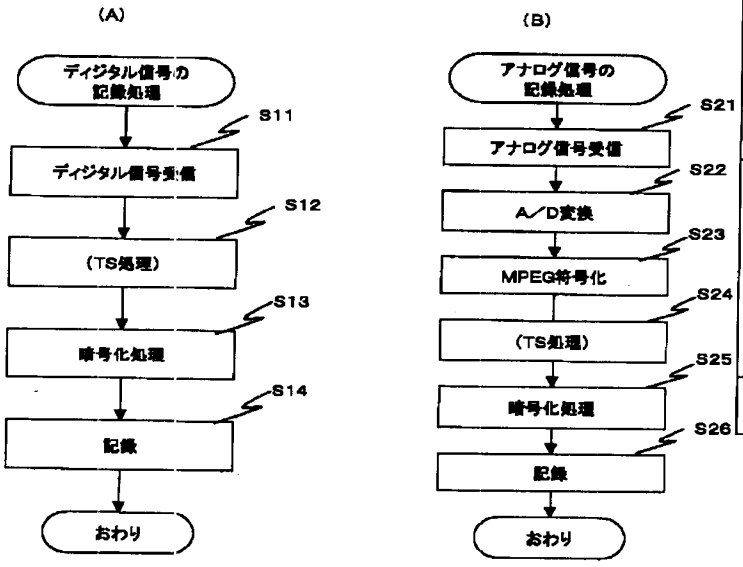
【図１８】



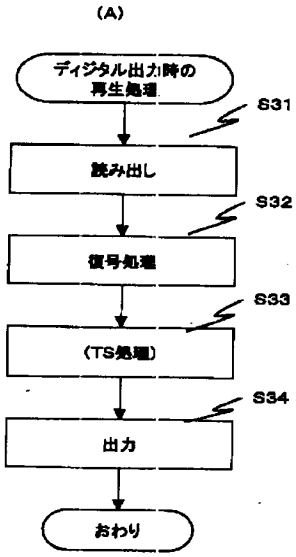

【図２０】

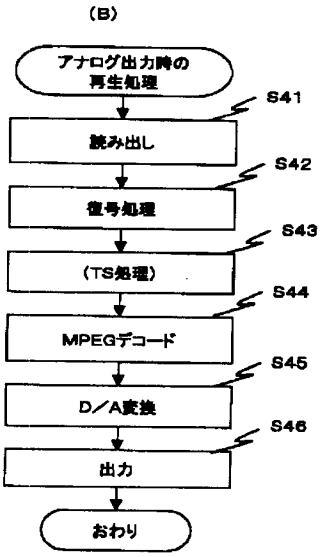
| | |
|---|---|
| ファイル1 | コンテンツデータのアドレス |
| | タイトルキーのアドレス |
| | デジタル署名のアドレス |
| | 公開鍵証明書のアドレス |
| | その他の情報 |
| ファイル2 | コンテンツデータのアドレス |
| | タイトルキーのアドレス |
| | デジタル署名のアドレス |
| | 公開鍵証明書のアドレス |
| | その他の情報 |
| ： | ： |

【図３】

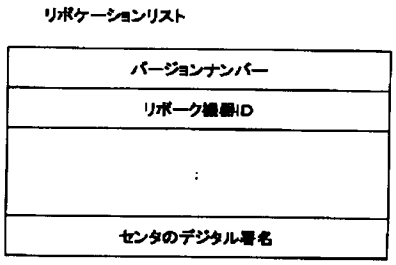


【図４】

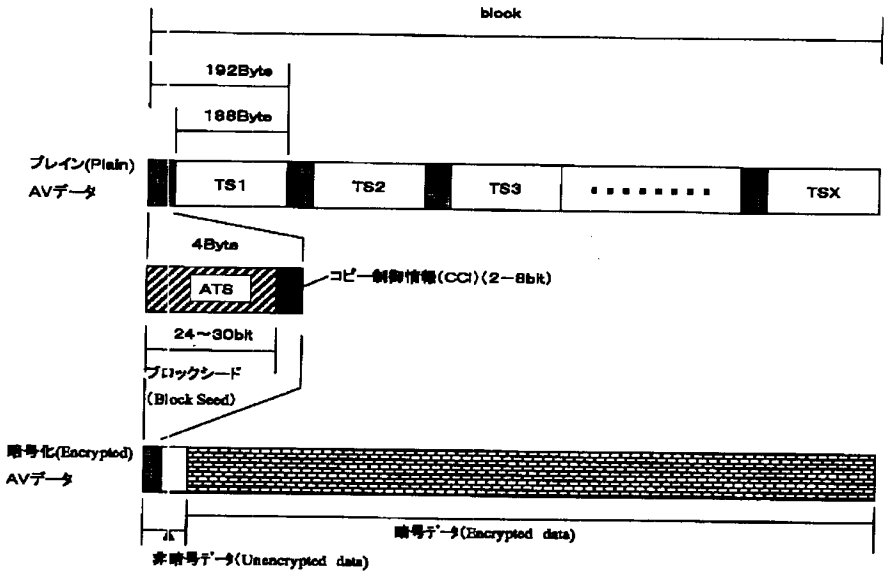

(A)
ディジタル出力時の再生処理
S31
読み出し
S32
復号処理
S33
(TS処理)
S34
出力
おわり


(B)
アナログ出力時の再生処理
S41
読み出し
S42
復号処理
S43
(TS処理)
S44
MPEGデコード
S45
D／A変換
S46
出力
おわり

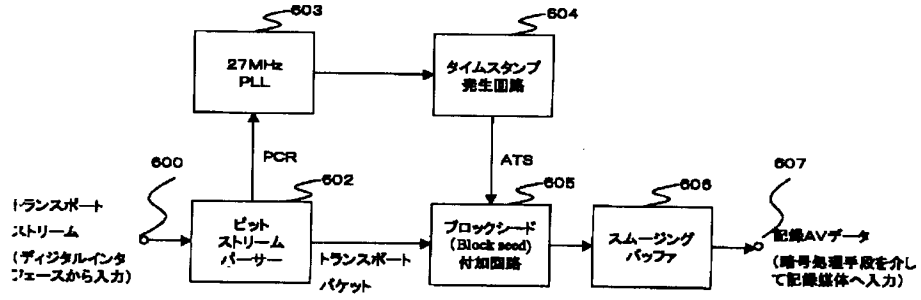
【図２３】


リポケーションリスト
バージョンナンバー
リポーク機器ID
:
センタのデジタル署名

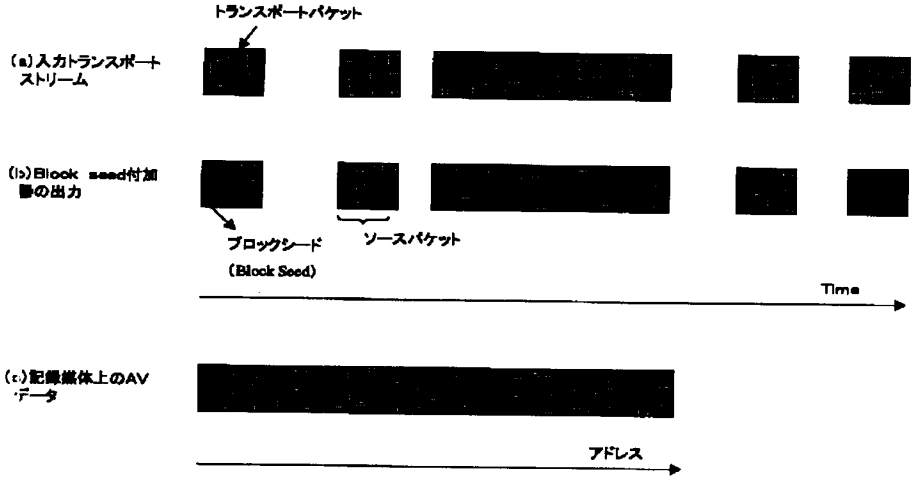
【図５】


block
192Byte
188Byte
プレイン(Plain)
AVデータ
TS1
TS2
TS3
TSX
4Byte
ATS
コピー制御情報(CCI)(2−8bit)
24〜30bit
ブロックシード
(Block Seed)
暗号化(Encrypted)
AVデータ
暗号データ(Encrypted data)
非暗号データ(Unencrypted data)

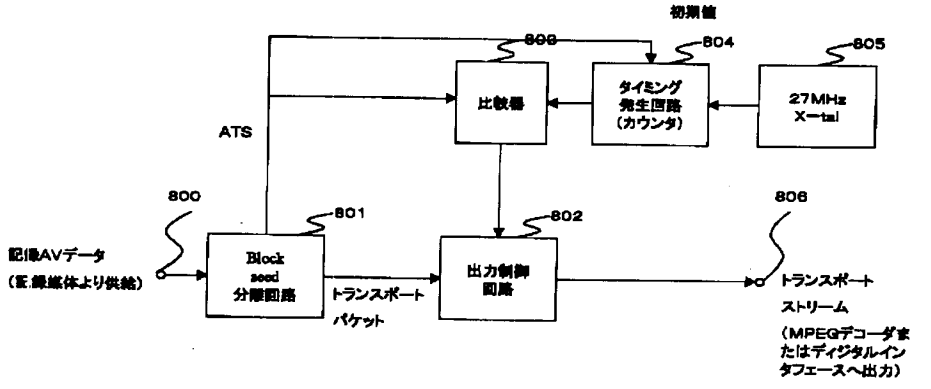
【図６】


603
27MHz PLL
604
タイムスタンプ発生回路
PCR
ATS
600
602
605
606
607
トランスポートストリーム（ディジタルインタフェースから入力）
ビットストリームパーサー
トランスポートパケット
ブロックシード（Block seed）付加回路
スムージングバッファ
記録AVデータ（暗号処理手段を介して記録媒体へ入力）

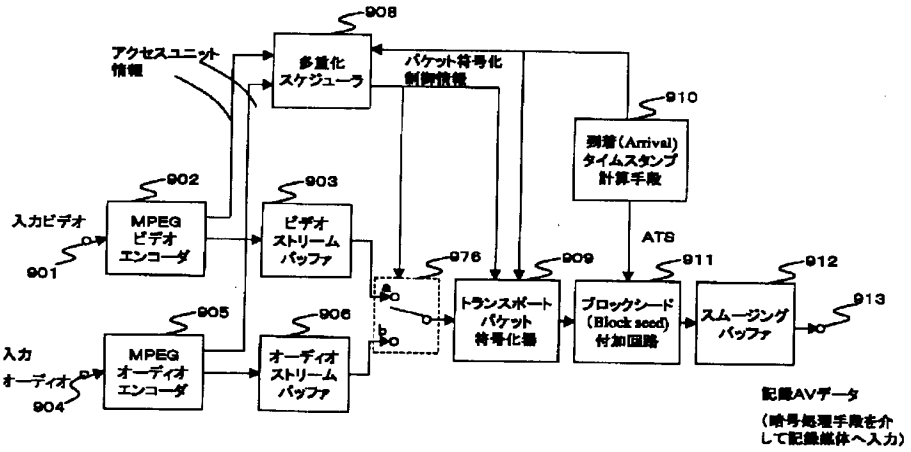
【図７】


トランスポートパケット
(a)入力トランスポートストリーム
(b)Block seed付加器の出力
ブロックシード（Block Seed）
ソースパケット
Time
(c)記録媒体上のAVデータ
アドレス

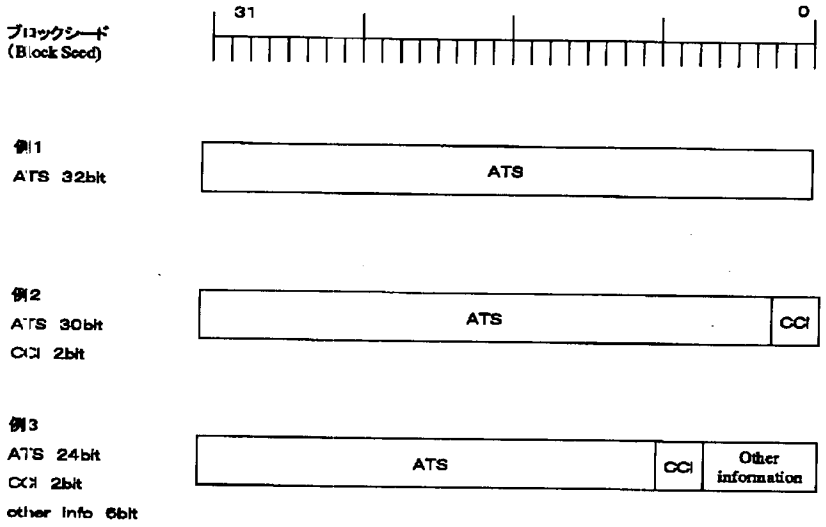
【図８】


初期値
803
804
805
比較器
タイミング発生回路（カウンタ）
27MHz X-tal
ATS
800
801
802
806
記録AVデータ（記録媒体より供給）
Block seed分離回路
トランスポートパケット
出力制御回路
トランスポートストリーム（MPEGデコーダまたはディジタルインタフェースへ出力）

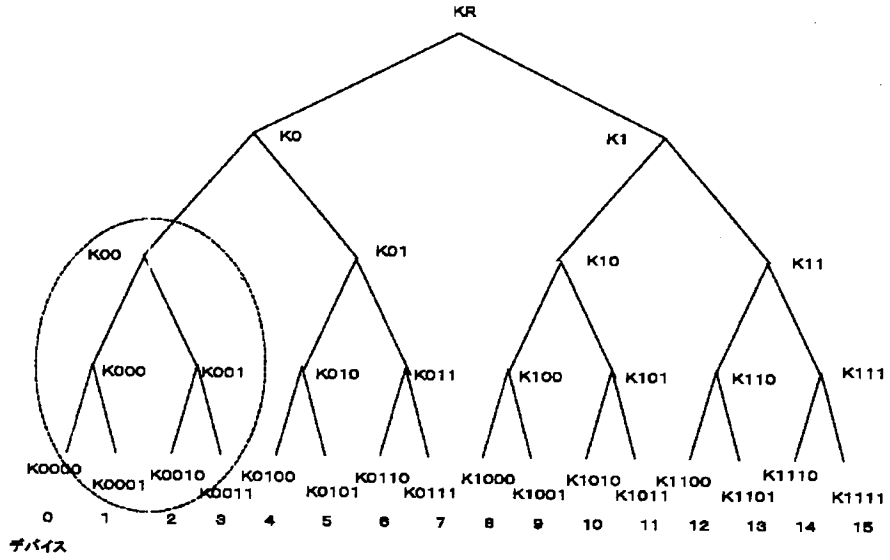
【図９】


908
アクセスユニット情報
多重化スケジューラ
パケット符号化制御情報
910
到着(Arrival)タイムスタンプ計算手段
902
903
入力ビデオ
MPEGビデオエンコーダ
ビデオストリームバッファ
901
976
909
911
912
ATS
905
906
913
入力オーディオ
MPEGオーディオエンコーダ
オーディオストリームバッファ
トランスポートパケット符号化器
ブロックシード(Block seed)付加回路
スムージングバッファ
904
記録AVデータ
(暗号処理手段を介して記録媒体へ入力)

【図１０】


ブロックシード
(Block Seed)
31
0
例1
ATS 32bit
ATS
例2
ATS 30bit
CCI 2bit
ATS
CCI
例3
ATS 24bit
CCI 2bit
other info 6bit
ATS
CCI
Other information

【図１１】




【図１２】

(A) 有効化キーブロック(EKB)　例1

デバイス0, 1, 2にt時点でのルートキーK(t)Rを送付

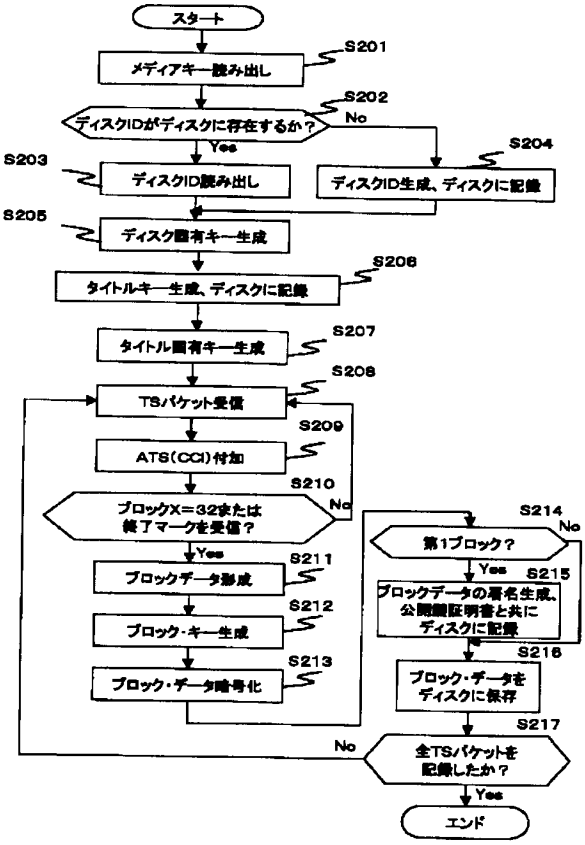
| 世代(Generation):t | |
|---|---|
| インデックス | 暗号化キー |
| 0 | Enc(K(t)0, K(t)R) |
| 00 | Enc(K(t)00, K(t)0) |
| 000 | Enc(K000, K(t)00) |
| 001 | Enc(K(t)001, K(t)00) |
| 0010 | Enc(K0010, K(t)001) |

(B) 有効化キーブロック(EKB)　例2

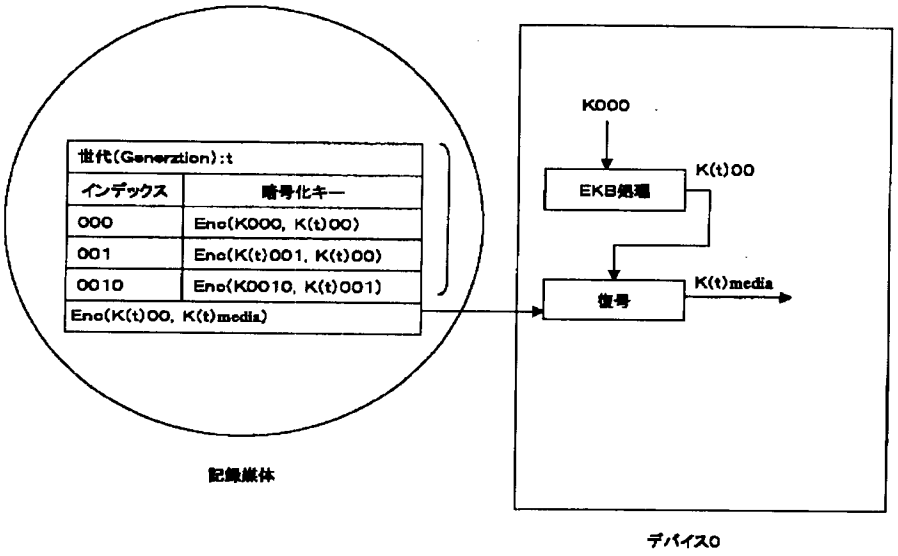
デバイス0, 1, 2にt時点でのルートキーK(t)Rを送付

| 世代(Generation):t | |
|---|---|
| インデックス | 暗号化キー |
| 000 | Enc(K000, K(t)00) |
| 001 | Enc(K(t)001, K(t)00) |
| 0010 | Enc(K0010, K(t)001) |

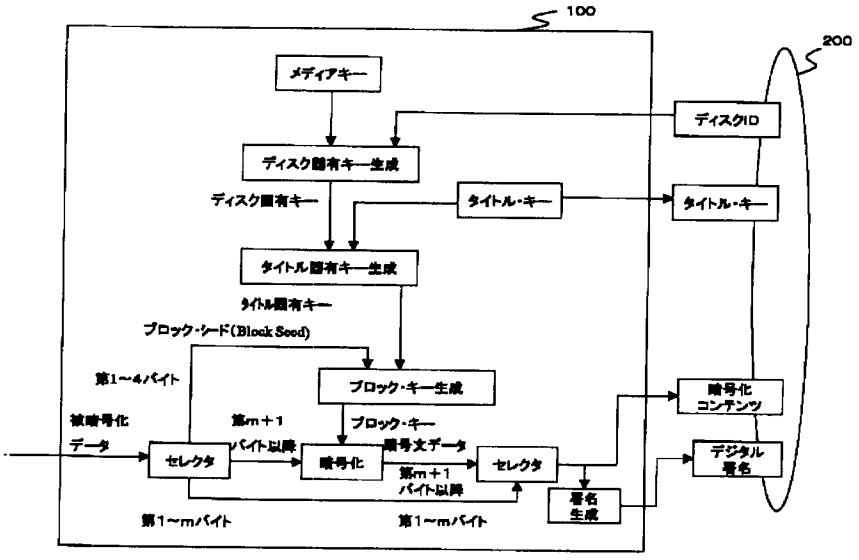
【図１９】



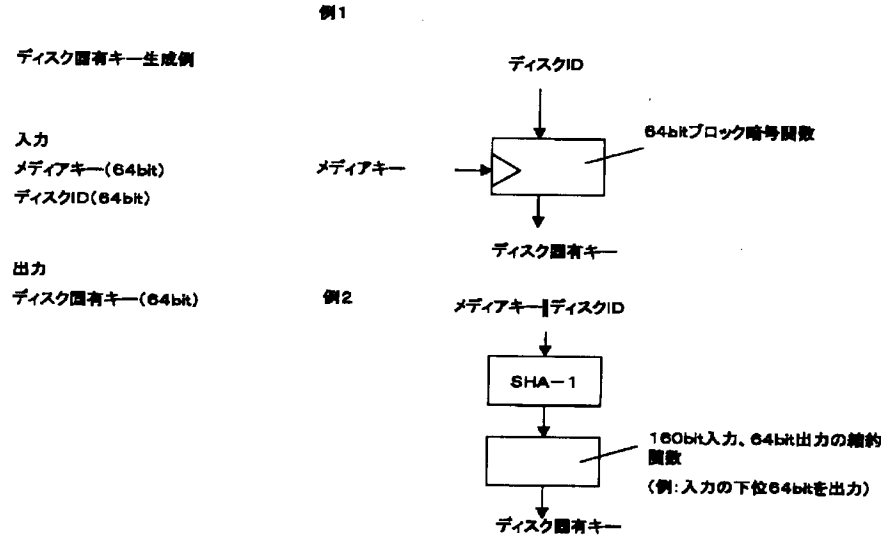
【図１３】


世代(Generation):t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)media)
記録媒体
K000
EKB処理
K(t)00
復号
K(t)media
デバイスD

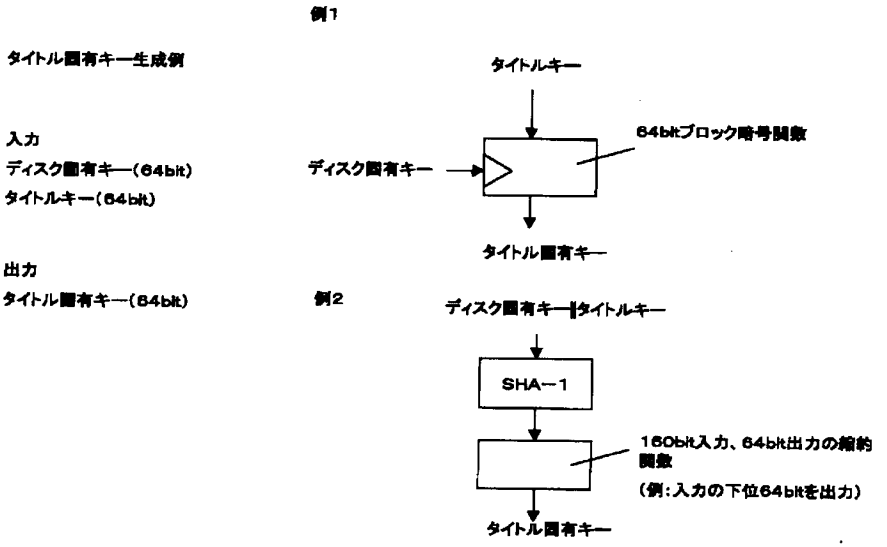
【図１４】


100
200
メディアキー
ディスクID
ディスク固有キー生成
ディスク固有キー
タイトル・キー
タイトル・キー
タイトル固有キー生成
タイトル固有キー
ブロック・シード(Block Seed)
第1～4バイト
ブロック・キー生成
暗号化コンテンツ
被暗号化データ
第m＋1バイト以降
ブロック・キー
セレクタ
暗号化
暗号文データ
第m＋1バイト以降
セレクタ
デジタル署名
署名生成
第1～mバイト
第1～mバイト

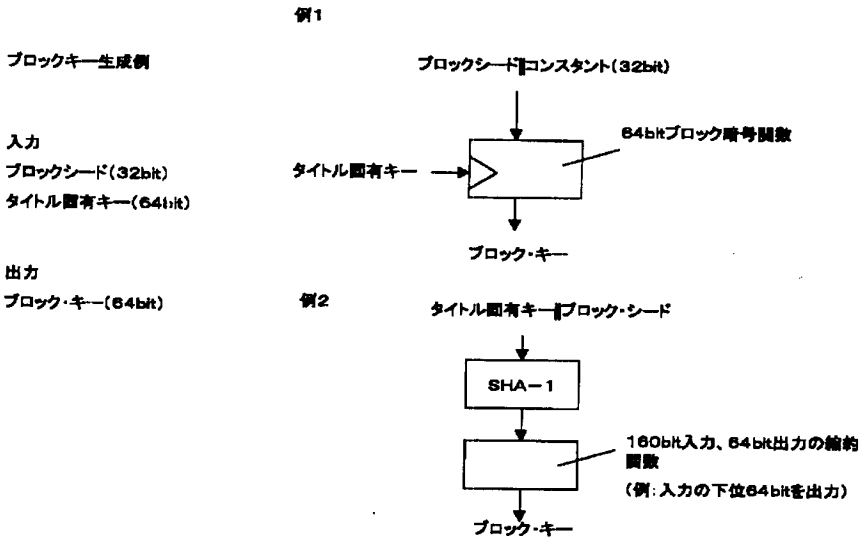
【図１５】


例1
ディスク固有キー生成例
入力
メディアキー(64bit)
ディスクID(64bit)
出力
ディスク固有キー(64bit)
ディスクID
メディアキー
64bitブロック暗号関数
ディスク固有キー
例2
メディアキー‖ディスクID
SHA－1
160bit入力、64bit出力の縮約関数
(例:入力の下位64bitを出力)
ディスク固有キー

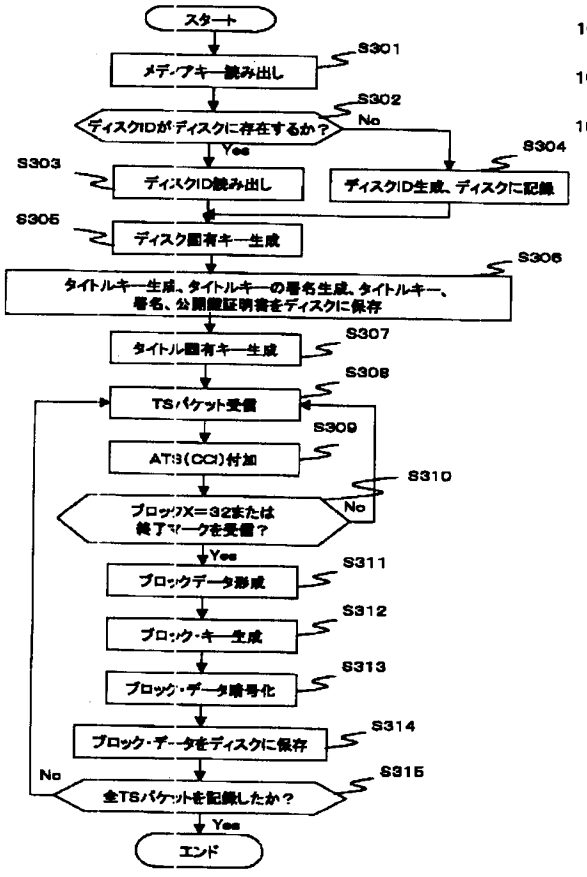
【図１６】


例1
タイトル固有キー生成例
入力
ディスク固有キー(64bit)
タイトルキー(64bit)
出力
タイトル固有キー(64bit)
タイトルキー
ディスク固有キー
64bitブロック暗号関数
タイトル固有キー
例2
ディスク固有キー‖タイトルキー
SHA－1
160bit入力、64bit出力の縮約関数
(例:入力の下位64bitを出力)
タイトル固有キー

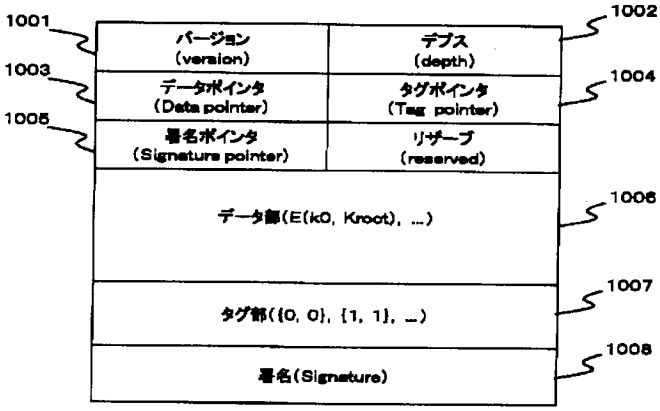
【図１７】


例1
ブロックキー生成例
ブロックシード‖コンスタント(32bit)
入力
ブロックシード(32bit)
タイトル固有キー(64bit)
タイトル固有キー
64bitブロック暗号関数
ブロック・キー
出力
ブロック・キー(64bit)
例2
タイトル固有キー‖ブロック・シード
SHA－1
160bit入力、64bit出力の縮約関数
(例：入力の下位64bitを出力)
ブロック・キー

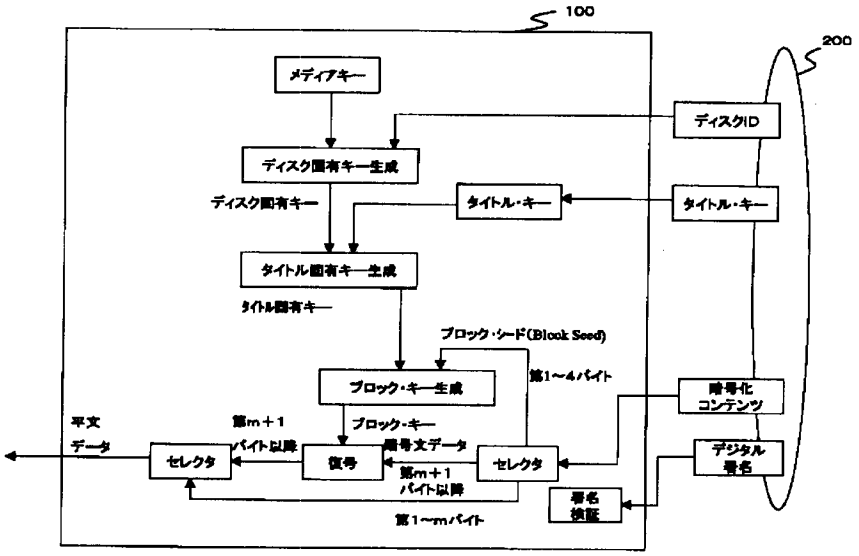
【図２１】


スタート
メディアキー読み出し
S301
ディスクIDがディスクに存在するか？
S302
No
Yes
S303
ディスクID読み出し
S304
ディスクID生成、ディスクに記録
S305
ディスク固有キー生成
S306
タイトルキー生成、タイトルキーの署名生成、タイトルキー、署名、公開鍵証明書をディスクに保存
タイトル固有キー生成
S307
S308
TSパケット受信
S309
ATS(CCI)付加
S310
ブロックX＝32または終了マークを受信？
No
Yes
S311
ブロックデータ形成
S312
ブロック・キー生成
S313
ブロック・データ暗号化
S314
ブロック・データをディスクに保存
S315
No
全TSパケットを記録したか？
Yes
エンド

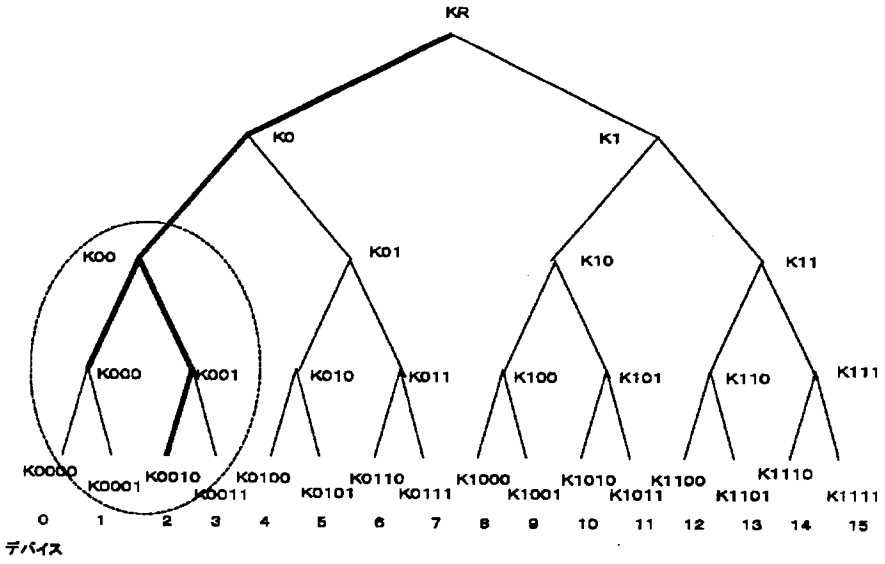
【図２５】


1001
1002
バージョン (version)
デプス (depth)
1003
1004
データポインタ (Data pointer)
タグポインタ (Tag pointer)
1005
署名ポインタ (Signature pointer)
リザーブ (reserved)
データ部(E(k0, Kroot), ...)
1006
タグ部({0, 0}, {1, 1}, ...)
1007
署名(Signature)
1008

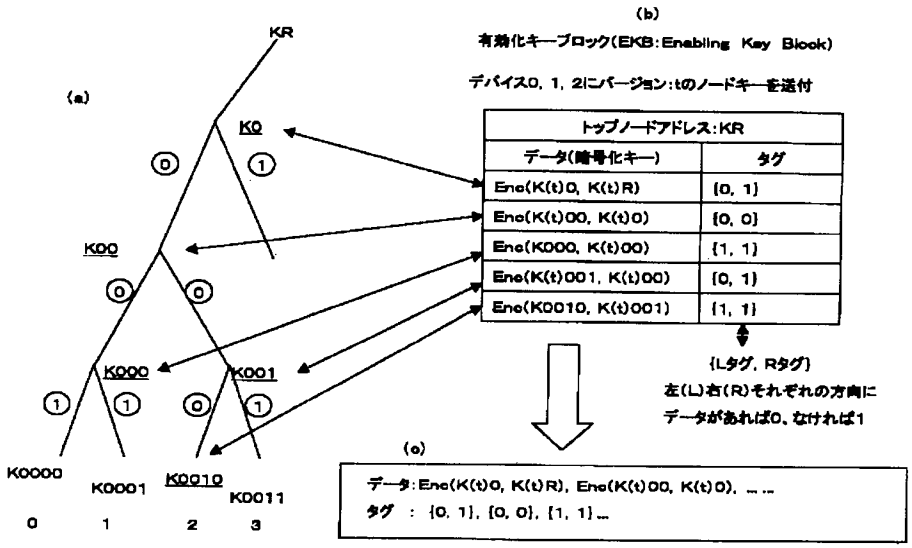
【図２２】


100
200
メディアキー
ディスクID
ディスク固有キー生成
ディスク固有キー
タイトル・キー
タイトル・キー
タイトル固有キー生成
タイトル固有キー
ブロック・シード(Block Seed)
第1～4バイト
ブロック・キー生成
暗号化コンテンツ
平文データ
第m＋1バイト以降
ブロック・キー
セレクタ
復号
暗号文データ
セレクタ
デジタル署名
第m＋1バイト以降
署名検証
第1～mバイト

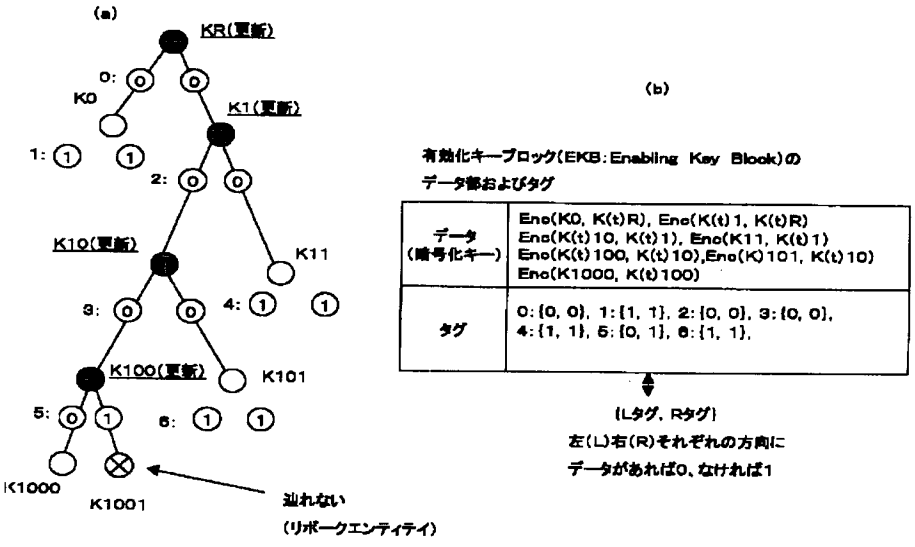
【図２４】


KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
デバイス

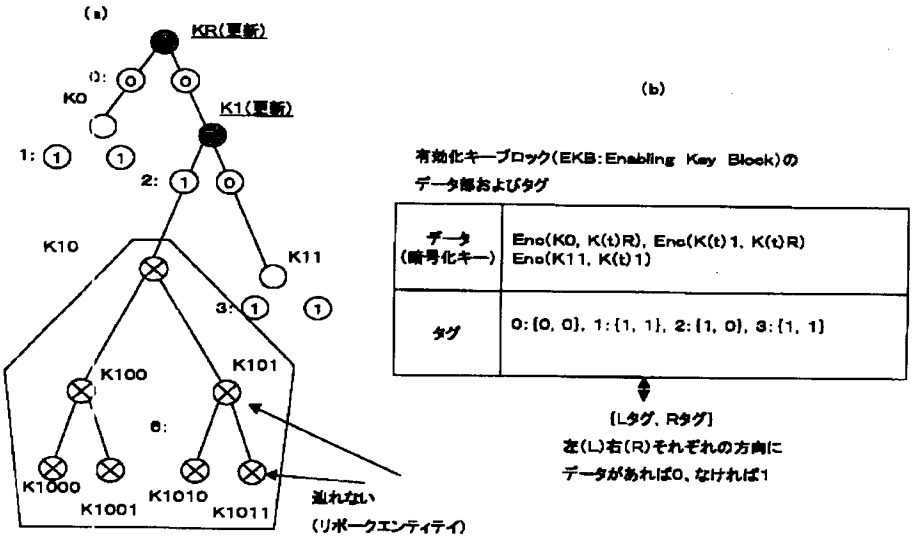
【図２６】


(a)
KR
K0
K00
K000
K001
K0000
K0001
K0010
K0011
0
1
2
3
(b)
有効化キーブロック(EKB:Enabling Key Block)
デバイス0, 1, 2にバージョン:tのノードキーを送付
トップノードアドレス:KR
データ(暗号化キー)
タグ
Enc(K(t)0, K(t)R)
{0, 1}
Enc(K(t)00, K(t)0)
{0, 0}
Enc(K000, K(t)00)
{1, 1}
Enc(K(t)001, K(t)00)
{0, 1}
Enc(K0010, K(t)001)
{1, 1}
{Lタグ, Rタグ}
左(L)右(R)それぞれの方向に
データがあれば0、なければ1
(c)
データ:Enc(K(t)0, K(t)R), Enc(K(t)00, K(t)0), ……
タグ : {0, 1}, {0, 0}, {1, 1}…

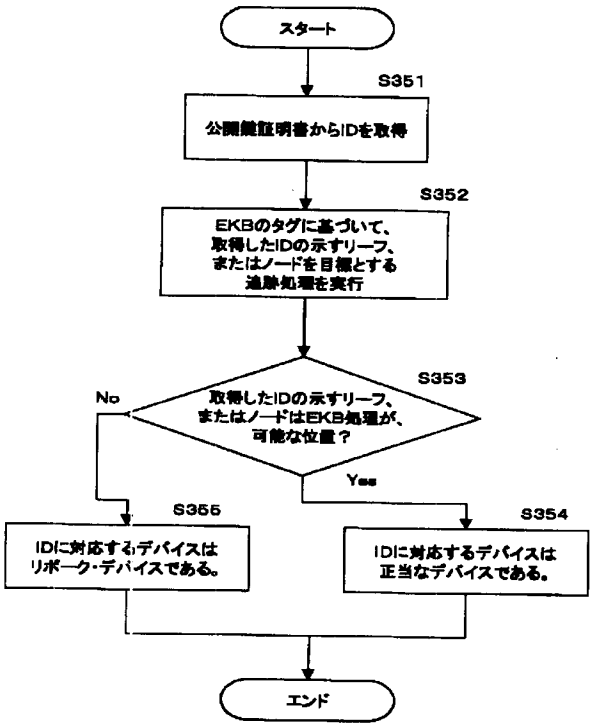
【図２７】


(a)
KR(更新)
0:
K0
K1(更新)
1:
2:
K10(更新)
K11
3:
4:
K100(更新)
K101
5:
6:
K1000
K1001
辿れない
(リボークエンティティ)
(b)
有効化キーブロック(EKB:Enabling Key Block)の
データ部およびタグ
データ
(暗号化キー)
Enc(K0, K(t)R), Enc(K(t)1, K(t)R)
Enc(K(t)10, K(t)1), Enc(K11, K(t)1)
Enc(K(t)100, K(t)10),Enc(K)101, K(t)10)
Enc(K1000, K(t)100)
タグ
0:{0, 0}, 1:{1, 1}, 2:{0, 0}, 3:{0, 0},
4:{1, 1}, 5:{0, 1}, 6:{1, 1},
{Lタグ, Rタグ}
左(L)右(R)それぞれの方向に
データがあれば0、なければ1

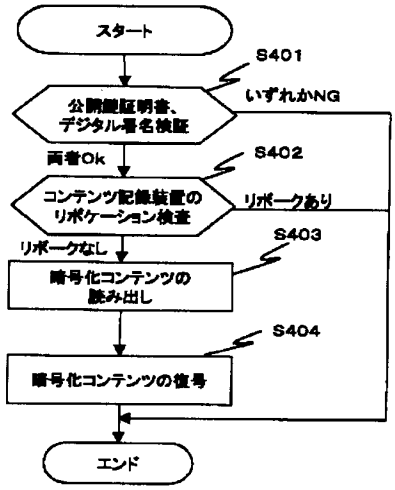
【図２８】


(a)
KR(更新)
0:
K0
K1(更新)
1:
2:
K10
K11
3:
K100
K101
e:
K1000
K1001
K1010
K1011
辿れない
(リボークエンティティ)
(b)
有効化キーブロック(EKB:Enabling Key Block)の
データ部およびタグ
データ
(暗号化キー)
Enc(K0, K(t)R), Enc(K(t)1, K(t)R)
Enc(K11, K(t)1)
タグ
0:{0, 0}, 1:{1, 1}, 2:{1, 0}, 3:{1, 1}
{Lタグ、Rタグ}
左(L)右(R)それぞれの方向に
データがあれば0、なければ1

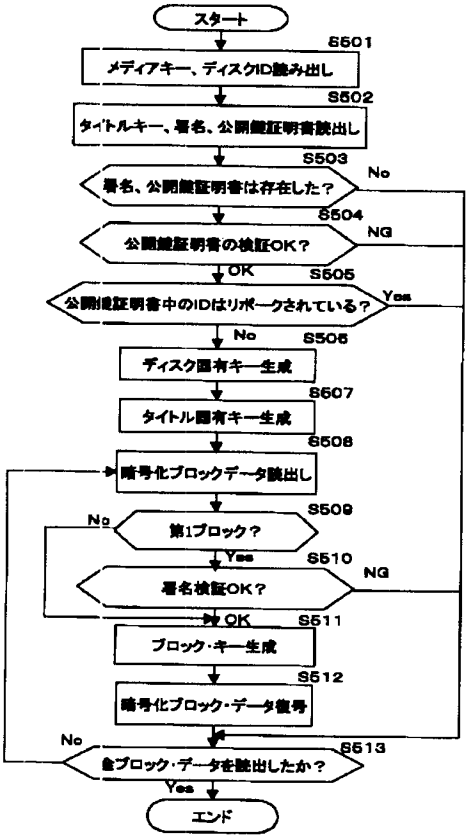
【図２９】


スタート
S351
公開鍵証明書からIDを取得
S352
EKBのタグに基づいて、
取得したIDの示すリーフ、
またはノードを目標とする
追跡処理を実行
S353
No
取得したIDの示すリーフ、
またはノードはEKB処理が、
可能な位置？
Yes
S355
IDに対応するデバイスは
リボーク・デバイスである。
S354
IDに対応するデバイスは
正当なデバイスである。
エンド

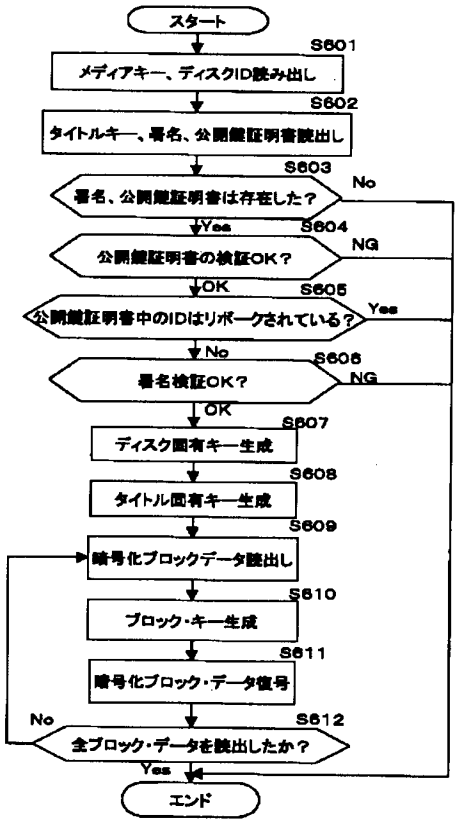
【図３０】


スタート
S401
公開鍵証明書、
デジタル署名検証
いずれかNG
両者Ok
S402
コンテンツ記録装置の
リボケーション検査
リボークあり
リボークなし
S403
暗号化コンテンツの
読み出し
S404
暗号化コンテンツの復号
エンド

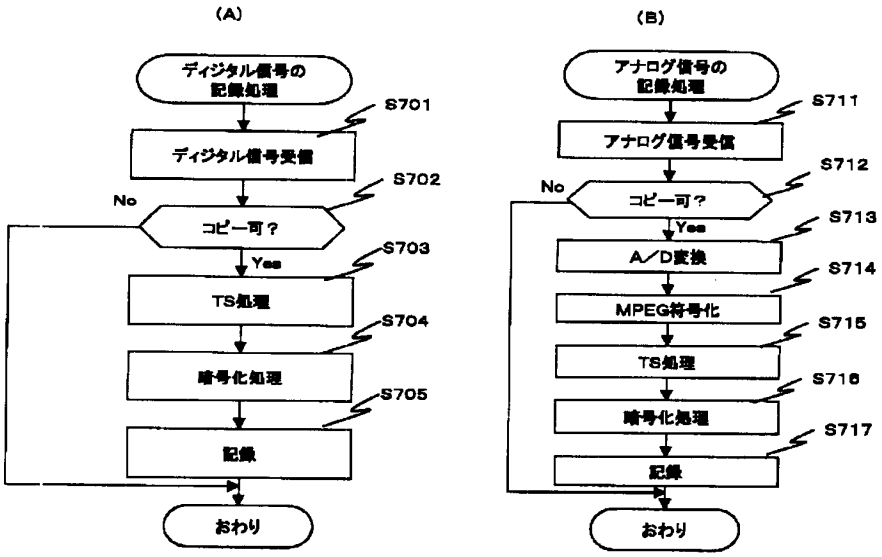
【図３１】


スタート
S501
メディアキー、ディスクID読み出し
S502
タイトルキー、署名、公開鍵証明書読出し
S503
署名、公開鍵証明書は存在した？
No
S504
公開鍵証明書の検証OK？
NG
OK
S505
公開鍵証明書中のIDはリボークされている？
Yes
No
S506
ディスク固有キー生成
S507
タイトル固有キー生成
S508
暗号化ブロックデータ読出し
S509
No
第1ブロック？
Yes
S510
署名検証OK？
NG
OK
S511
ブロック・キー生成
S512
暗号化ブロック・データ復号
No
S513
全ブロック・データを読出したか？
Yes
エンド

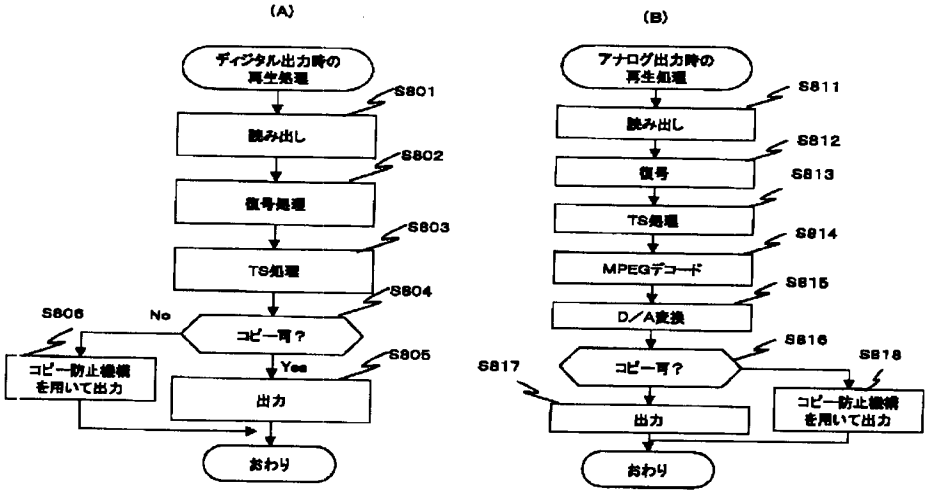
【図３２】


スタート
S601
メディアキー、ディスクID読み出し
S602
タイトルキー、署名、公開鍵証明書読出し
S603
署名、公開鍵証明書は存在した？
No
Yes
S604
公開鍵証明書の検証OK？
NG
OK
S605
公開鍵証明書中のIDはリボークされている？
Yes
No
S606
署名検証OK？
NG
OK
S607
ディスク固有キー生成
S608
タイトル固有キー生成
S609
暗号化ブロックデータ読出し
S610
ブロック・キー生成
S611
暗号化ブロック・データ復号
No
S612
全ブロック・データを読出したか？
Yes
エンド

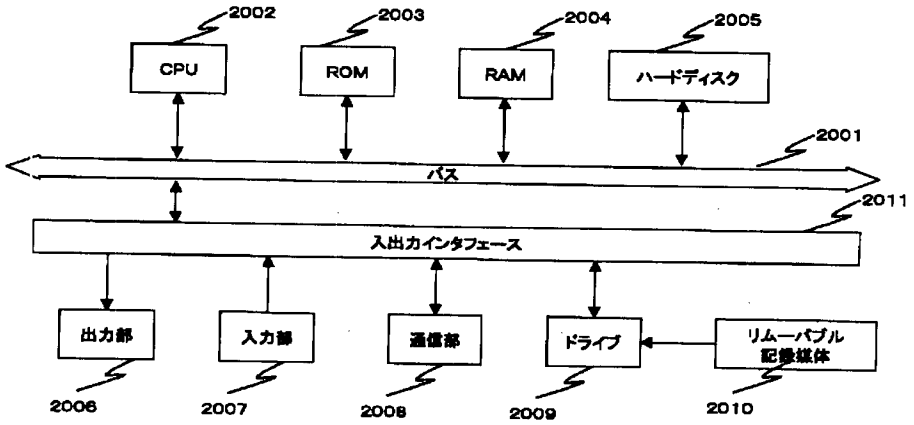
【図３３】


(A)
ディジタル信号の記録処理
S701
ディジタル信号受信
S702
No
コピー可？
Yes
S703
TS処理
S704
暗号化処理
S705
記録
おわり
(B)
アナログ信号の記録処理
S711
アナログ信号受信
S712
No
コピー可？
Yes
S713
A／D変換
S714
MPEG符号化
S715
TS処理
S716
暗号化処理
S717
記録
おわり

【図３４】

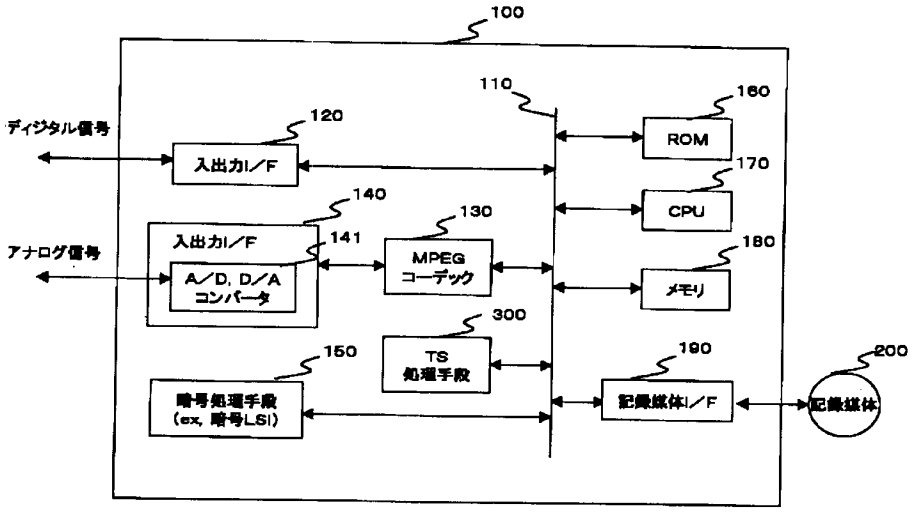



【図３５】




---

【手続補正書】
【提出日】平成１４年２月５日（２００２．２．５）
【手続補正１】
【補正対象書類名】図面
【補正対象項目名】図１
【補正方法】変更
【補正内容】
【図１】


100
110
160
ROM
120
ディジタル信号
入出力I／F
170
CPU
140
入出力I／F
130
141
アナログ信号
A／D, D／A
コンバータ
MPEG
コーデック
180
メモリ
300
TS
処理手段
150
190
200
暗号処理手段
(ex, 暗号LSI)
記録媒体I／F
記録媒体